Manuale Operativo

Posta Elettronica Certificata

Regione Basilicata

Redazione	Giuseppe Bernardo
Versione	REV.2
Data	18/05/2016

INDICE

INDICE DELLE FIGURE

1 – GENERALITÀ

1.1 Scopo

Il presente documento descrive le modalità di utilizzo del servizio di Posta Elettronica Certificata (PEC) erogato dalla Regione Basilicata attraverso la struttura operativa dell'Ufficio Società dell'informazione.

Il Manuale Operativo definisce le regole e descrive le procedure utilizzate dal Gestore di PEC per l'erogazione del servizio. Il documento è pubblicato per garantire la massima trasparenza nei confronti dei clienti del servizio e degli altri Gestori.

1.2 Versione del manuale e responsabilità

La Regione Basilicata è responsabile della stesura del presente documento.

La versione del documento e le singole responsabilità dei redattori e supervisori sono riportate nella matrice delle revisioni in copertina.

1.3 Tabella di corrispondenza

Riportiamo qui di seguito la tabella di corrispondenza tra i paragrafi del presente documento e gli argomenti contenuti nella CIRCOLARE n. 56 del 21 maggio 2009.

Punto	Circolare CNIPA	Paragrafo
a)	Dati identificativi del gestore	3 –
b)	Indicazione del responsabile del manuale	3.2
c)	Riferimenti normativi necessari per la verifica dei contenuti	2 –
d)	Indirizzo del sito web del gestore ove il manuale è pubblicato e scaricabile	3.5
f)	Le definizioni relative alle abbreviazioni e ai termini tecnici che in esso figurano	1.4
g)	La descrizione e le modalità del servizio offerto	5 –

Punto	Circolare CNIPA	Paragrafo
h)	La descrizione delle modalità di reperimento e di presentazione delle informazioni presenti nei log dei messaggi	5.6
i)	Le modalità di accesso e di fornitura del servizio	5 – -5.3 - 7 –
j)	I livelli di servizio e i relativi indicatori di qualità di cui all'articolo 12 del decreto del Ministro per l'innovazione e le tecnologie 2 novembre 2005	7.2
k)	Le modalità di protezione dei dati dei titolari delle caselle, gli obblighi e le responsabilità che ne discendono, le esclusioni e le eventuali limitazioni in caso di indennizzo, relativamente ai soggetti previsti all'articolo 2 del decreto del Presidente della Repubblica n. 68/2005	9 – - 10 –
l)	Le procedure operative da attuare nel caso di cessazione dell'attività di gestore di Posta Elettronica Certificata	5.11
m)	La versione del medesimo manuale	Pag1

1.4 Definizioni ed acronimi

PEC	*Posta Elettronica Certificata*
DigitPA	*ente nazionale per la digitalizzazione della pubblica amministrazione*
Open Source	*In informatica, Open Source indica un software rilasciato con un tipo di licenza per la quale il codice sorgente è lasciato alla disponibilità di eventuali sviluppatori, in modo che con la collaborazione (in genere libera e spontanea) il prodotto finale possa raggiungere una complessità maggiore di quanto potrebbe ottenere un singolo gruppo di programmazione*
Gestore di	*E' il soggetto che gestisce uno o più domini di posta elettronica certificata*

posta elettronica certificata	*con i relativi punti di accesso, di ricezione e di consegna, titolare della chiave usata per la firma delle ricevute e delle buste e che si interfaccia con altri gestori di posta elettronica certificata per l'interoperabilità con altri titolari;*
Titolare	*E' il soggetto a cui é assegnata una casella di posta elettronica certificata*
Dominio di posta elettronica certificata	*E' un dominio di posta elettronica certificata che contiene unicamente caselle di posta elettronica certificata*
Indice dei gestori di posta elettronica certificata	*E' il sistema, che contiene l'elenco dei domini e dei gestori di posta elettronica certificata, con i relativi certificati corrispondenti alle chiavi usate per la firma delle ricevute, degli avvisi e delle buste, realizzato per mezzo di un server Lightweight Directory Access Protocol, di seguito denominato LDAP, posizionato in un'area raggiungibile dai vari gestori di posta elettronica certificata e che costituisce, inoltre, la struttura tecnica relativa all'elenco pubblico dei gestori di posta elettronica certificata*
Casella di posta elettronica certificata	*E' la casella di posta elettronica posta all'interno di un dominio di posta elettronica certificata ed alla quale é associata una funzione che rilascia ricevute di avvenuta consegna al ricevimento di messaggi di posta elettronica certificata*
HTML	*HTML (acronimo per HyperText Mark-Up Language) è un linguaggio usato per descrivere i documenti ipertestuali disponibili su Internet. Non è un linguaggio di programmazione, ma un linguaggio di markup, ossia descrive il contenuto, testuale e non, di una pagina web*
MTA	*Mail Transfer Agent. E' un modulo che ha il compito di effettuare il dispatching dei messaggi di posta elettronica (invio e ricezione)*
LDAP	*Lightweight Directory Access Protocol. E' un protocollo di rete utilizzato per la ricerca e memorizzazione di informazioni su un Directory Server. Un directory server LDAP è un albero di entità costituite da attributi e valori. Un classico utilizzo di un directory server è la memorizzazioni degli account email o degli utenti registrati ad un sito*
SNMP	*Simple Network Management Protocol. E' un protocollo utilizzato per la gestione ed il monitoring degli apparati di rete*
HSM	*Hardware Security Module. E' un dispositivo hardware per la generazione, la memorizzazione e la protezione sicura di chiavi crittografiche.*
NTP	*Network Time Protocol*
SMTP	*Simple Mail Transfer Protocol. Protocollo Standard per la trasmissione di*

	email su internet
SMTP/S	*Protocollo SMTP, che consente l'accesso al servizio di posta elettronica mediante l'uso dei protocolli TLS Transport Layer Security (TLS) o Secure Sockets Layer (SSL) per la cifratura della comunicazione.* *La porta di comunicazione comunemente utilizzata è la TCP 465.*
POP3	*Post Office Protocol. Protocollo per l'accesso ad un account di posta elettronica* *La porta di comunicazione comunemente utilizzata è la TCP 110*
POP3/S	*Protocollo POP3, che consente l'accesso al servizio di posta elettronica mediante l'uso dei protocolli TLS Transport Layer Security (TLS) o Secure Sockets Layer (SSL) per la cifratura della comunicazione.* *La porta di comunicazione comunemente utilizzata è la TCP 995.*
IMAP	*Internet Message Access Protocol. Protocollo per l'accesso ad un account di posta elettronica e per la lettura delle email.* *La porta di comunicazione comunemente utilizzata è la TCP 143*
IMAP/S	*Protocollo IMAP, che consente l'accesso al servizio di posta elettronica mediante l'uso dei protocolli TLS Transport Layer Security (TLS) o Secure Sockets Layer (SSL) per la cifratura della comunicazione.* *La porta di comunicazione comunemente utilizzata è la TCP 993.*
LMTP	*Local Mail Transfer Protocol. Derivato dall'SMTP, lo può sostituire nei casi in cui il ricevente non gestisce la coda dei messaggi.*
CTT	*Centro Tecnico Territoriale (centro servizi). E' il centro attraverso il quale Regione Basilicata eroga il servizio di posta elettronica certificata.*
Punto di accesso	*E' il sistema che fornisce i servizi di accesso per l'invio e la lettura di messaggi di posta elettronica certificata, nonché i servizi di identificazione ed accesso dell'utente, di verifica della presenza di virus informatici all'interno del messaggio, di emissione della ricevuta di accettazione e di imbustamento del messaggio originale nella busta di trasporto*
Punto di ricezione	*E' il sistema che riceve il messaggio all'interno di un dominio di posta elettronica certificata, effettua i controlli sulla provenienza e sulla correttezza del messaggio ed emette la ricevuta di presa in carico, imbusta i messaggi errati in una busta di anomalia e verifica la presenza di virus informatici all'interno dei messaggi di posta ordinaria e delle buste di trasporto*
Punto di	*E' il sistema che compie la consegna del messaggio nella casella di posta*

consegna	*elettronica certificata del titolare destinatario, verifica la provenienza e la correttezza del messaggio ed emette, a seconda dei casi, la ricevuta di avvenuta consegna o l'avviso di mancata consegna*
Firma del gestore di posta elettronica certificata	*E' la firma elettronica avanzata, basata su un sistema di chiavi asimmetriche, che consente di rendere manifesta la provenienza e di assicurare l'integrità e l'autenticità dei messaggi del sistema di posta elettronica certificata, generata attraverso una procedura informatica che garantisce la connessione univoca al gestore e la sua univoca identificazione, creata automaticamente con mezzi che garantiscano il controllo esclusivo da parte del gestore*
Ricevuta di accettazione	*E' la ricevuta, sottoscritta con la firma del gestore di posta elettronica certificata del mittente, contenente i dati di certificazione, rilasciata al mittente dal punto di accesso a fronte dell'invio di un messaggio di posta elettronica certificata*
Avviso di non accettazione	*E' l'avviso, sottoscritto con la firma del gestore di posta elettronica certificata del mittente, che viene emesso quando il gestore mittente é impossibilitato ad accettare il messaggio in ingresso, recante la motivazione per cui non é possibile accettare il messaggio e l'esplicitazione che il messaggio non potrà essere consegnato al destinatario*
Ricevuta di presa in carico	*E' la ricevuta, sottoscritta con la firma del gestore di posta elettronica certificata del destinatario, emessa dal punto di ricezione nei confronti del gestore di posta elettronica certificata mittente per attestare l'avvenuta presa in carico del messaggio da parte del sistema di posta elettronica certificata di destinazione, recante i dati di certificazione per consentirne l'associazione con il messaggio a cui si riferisce;*
Ricevuta di avvenuta consegna	*E' la ricevuta, sottoscritta con la firma del gestore di posta elettronica certificata del destinatario, emessa dal punto di consegna al mittente nel momento in cui il messaggio é inserito nella casella di posta elettronica certificata del destinatario*
Ricevuta completa di avvenuta consegna	*E' la ricevuta nella quale sono contenuti i dati di certificazione ed il messaggio originale*
Ricevuta breve di avvenuta consegna	*E' la ricevuta nella quale sono contenuti i dati di certificazione ed un estratto del messaggio originale*

Ricevuta sintetica di avvenuta consegna	*E' la ricevuta che contiene i dati di certificazione*
Avviso di mancata consegna	*E' l'avviso, emesso dal sistema, per indicare l'anomalia al mittente del messaggio originale nel caso in cui il gestore di posta elettronica certificata sia impossibilitato a consegnare il messaggio nella casella di posta elettronica certificata del destinatario*
Messaggio originale	*E' il messaggio inviato da un utente di posta elettronica certificata prima del suo arrivo al punto di accesso e consegnato al titolare destinatario per mezzo di una busta di trasporto che lo contiene*
Busta di trasporto	*E' la busta creata dal punto di accesso e sottoscritta con la firma del gestore di posta elettronica certificata mittente, all'interno della quale sono inseriti il messaggio originale inviato dall'utente di posta elettronica certificata ed i relativi dati di certificazione*
Busta di anomalia	*E' la busta, sottoscritta con la firma del gestore di posta elettronica certificata del destinatario, nella quale é inserito un messaggio errato ovvero non di posta elettronica certificata e consegnata ad un titolare, per evidenziare al destinatario detta anomalia*
Dati di certificazione	*Sono i dati, quali ad esempio data ed ora di invio, mittente, destinatario, oggetto, identificativo del messaggio, che descrivono l'invio del messaggio originale e sono certificati dal gestore di posta elettronica certificata del mittente; tali dati sono inseriti nelle ricevute e sono trasferiti al titolare destinatario insieme al messaggio originale per mezzo di una busta di trasporto*
Marca temporale	*E' un'evidenza informatica con cui si attribuisce, ad uno o più documenti informatici, un riferimento temporale opponibile ai terzi secondo quanto previsto dal decreto del Presidente della Repubblica 28 dicembre 2000, n. 445 e dal decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004, pubblicato nella Gazzetta Ufficiale n. 98 del 27 aprile 2004*
Tamper-evidence	*E' un sistema per segnalare qualsiasi tentativo di manomissione fisica del server che possa aver compromesso l'integrità del sistema e/o dei dati in esso contenuti; tipicamente realizzato tramite l'apposizione sulle macchine di sigilli, lucchetti, etichette autoadesive e/o qualsiasi altro mezzo di protezione il cui stato, in caso di accesso non autorizzato, risulti evidentemente compromesso ad un osservatore esterno*
Tamper-proof hardware	*E' un sistema di protezione fisica del server allo scopo di prevenire/impedire l'accesso e la manomissione del sistema dati da parte*

	di soggetti non autorizzati

2 – RIFERIMENTI DI LEGGE

Nella tabella di seguito riportata sono indicati i riferimenti normativi del presente manuale.

Normativa	
DPR 445/2000	Decreto del Presidente della Repubblica N. 445 del 28/12/2000: Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa. (Testo A)." (G.U. n. 42 del 20 Febbraio 2000 - Supplemento ordinario n. 30) e sue modificazioni secondo DPR 137/2003
Codice Privacy	Decreto legislativo n. 196 del 30 giugno 2003 “Codice in materia di protezione dei dati personali”. (G.U. n. 174 del 29 Luglio 2003)
DPR 68/2005	Decreto del Presidente della Repubblica 11 Febbraio 2005 n. 68, “Regolamento recante disposizioni per l'utilizzo della Posta Elettronica Certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3”, (G.U. n. 97 del 28 aprile 2005)
CAD	Decreto legislativo 7 Marzo 2005, n. 82 “Codice dell'Amministrazione Digitale" (G.U. n. 112 del 16 Maggio 2005) e s.m.i.
DM 2/11/2005	Decreto Ministeriale del 2 novembre 2005: “Regole tecniche per la formazione, la trasmissione, la validazione, anche temporale, della posta elettronica certificata” (G.U. n. 266 del 15 novembre 2005)
CNIPA/CR/51/2006	Circolare CNIPA del 7 dicembre 2006, n. 51 n. CNIPA/CR/51 “Espletamento della vigilanza e del controllo sulle attività esercitate dagli iscritti nell'elenco dei gestori di Posta Elettronica Certificata (PEC), di cui all'articolo 14 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68, «Regolamento recante disposizioni per l'utilizzo della Posta

Normativa	
	Elettronica Certificata, a norma dell'articolo 27 della legge 16 gennaio 2003, n. 3»”
CNIPA/CR/56/2009	Circolare CNIPA del 21 maggio 2009 n. CNIPA/CR/56 “Modalità per la presentazione delle domande di iscrizione nell’elenco pubblico dei gestori di Posta Elettronica Certificata (PEC) di cui all’art. 14 del decreto del Presidente della Repubblica 11 febbraio 2005, n. 68”.
Legge 2/2009	Legge di conversione, con modificazioni, del decreto-legge 29 novembre 2008, n. 185, recante misure urgenti per il sostegno a famiglie, lavoro, occupazione e impresa e per ridisegnare in funzione anti-crisi il quadro strategico nazionale"

3 – INFORMAZIONI SUL GESTORE

Il servizio di Posta Elettronica Certificata verrà erogato da Regione Basilicata del quale riportiamo nel seguito tutte le informazioni identificative.

Dati identificativi del gestore	
Ragione Sociale:	Regione Basilicata
Sede Legale:	Via Vincenzo Verrastro 4, 85100 Potenza
Sedi di erogazione del servizio:	Regione Basilicata Via Vincenzo Verrastro 4, 85100 – Potenza (PZ) Tel: 800.29.20.20
Partita IVA:	80002950766
Sito web:	http://pec.basilicatanet.it
email:	AOO-giunta@cert.regione.basilicata.it

3.1 Progetto Basilicata PEC

Il progetto **Basilicata PEC**, rientra tra gli interventi strategici del PO FESR 2007-2013.

Il PO FESR 2007-2013 attraverso l'Asse II "Società della conoscenza" persegue l'obiettivo generale di fare della Basilicata una società incentrata sulla "economia della conoscenza" attraverso il potenziamento della ricerca, la diffusione delle innovazioni e lo sviluppo del settore ICT.

In particolare la Linea di Intervento II.2.1.B del PO FESR prevede il miglioramento degli standard di accessibilità e sicurezza, funzionalità ed operatività alla rete mediante l'adozione di tecnologie dell'informazione e della comunicazione mirati a garantire, agli utenti residenti, i diritti propri della 'cittadinanza elettronica'.

La Regione Basilicata intende accreditarsi presso il DigitPA per diventare soggetto gestore del servizio di Posta Elettronica Certificata.

In questo modo l'ente erogherà il servizio di PEC attraverso il portale Basilicatanet, rivolgendo la propria offerta a cittadini residenti nella regione Basilicata (persone fisiche e giuridiche) ed alle pubbliche amministrazioni connesse alla rete RUPAR.

L'obiettivo verrà raggiunto attraverso la realizzazione di due interventi:

1. Affidamento diretto in favore della Ditta ARUBA PEC S.p.a. per la messa in opera di un sistema di Posta Elettronica Certificata;

2. Affidamento diretto in favore della Ditta TAB s.r.l. per la certificazione dell'erogazione dei servizi di Posta Elettronica Certificata della Regione Basilicata.

3.2 Responsabile del Manuale Operativo

Il responsabile della stesura e del mantenimento del presente manuale operativo è: Dott. BERNARDO .

Il responsabile può essere contattato ai recapiti

tel: 0971 666626

e-mail: giuseppe.bernardo@regione.basilicata.it

3.3 Canali di comunicazione

Oltre al riferimento indicato nel precedente paragrafo, il cliente può contattare la Regione Basilicata attraverso i canali di seguito specificati.

Sito internet della Regione Basilicata sulla PEC: http://pec.basilicatanet.it;

Numero Verde Contact Center: 800.29.20.20

3.3.1 Assistenza sul servizio

Per assistenza sul funzionamento del sistema e su eventuali malfunzionamenti è possibile mettersi in contatto con il fornitore del servizio con i seguenti mezzi:

Sito internet della Regione Basilicata sulla PEC:http://pec.basilicatanet.it;

Numero Verde Contact Center: 800.29.20.20

3.4 Modifiche al manuale

Il presente manuale potrà subire modifiche dettate dalla necessità di adattare il sistema a nuove normative che verranno emesse da parte degli organi competenti. Il manuale potrà inoltre aggiornato in caso di modifiche ed ottimizzazioni al sistema o cambiamenti relativi alle modalità di erogazione del servizio e dell'offerta da parte della Regione Basilicata.

La Regione Basilicata garantisce in qualsiasi momento la coerenza del manuale con la versione del sistema.

Tutte le future modifiche del Manuale verranno sottoposte a verifica ed approvazione interna (ad opera dei responsabili del servizio) ed esterna (ad opera del DigitPA) prima di essere pubblicate.

3.5 Indirizzo web del gestore dal quale scaricare il manuale

All'interno del sito web del gestore http://pec.basilicatanet.it è disponibile la copia in formato pdf del presente documento.

Il file può essere scaricato all'indirizzo: http://pec.basilicatanet.it

La Regione Basilicata garantisce che sul sito sia sempre pubblicata l'ultima versione esistente del manuale operativo.

4 – INTRODUZIONE: LA POSTA ELETTRONICA CERTIFICATA

*La **Posta Elettronica Certificata (PEC)** è un sistema di posta elettronica nel quale al mittente viene fornita documentazione elettronica, con valenza legale, attestante l'invio e la consegna di documenti informatici.*

La PEC è nata con l'obiettivo di trasferire su digitale il concetto di *Raccomandata con Ricevuta di Ritorno*. Come mezzo di trasporto si è scelto di utilizzare l'email che garantisce, oltre alla facilità di utilizzo e alla diffusione capillare sul territorio, una velocità di consegna non paragonabile alla posta tradizionale.

Attraverso la PEC chi invia una email ha la certezza dell'avvenuta (o mancata) consegna del proprio messaggio e dell'eventuale documentazione allegata.

Per certificare l'avvenuta consegna vengono utilizzate delle ricevute che costituiscono prova legale dell'avvenuta spedizione del messaggio e dell'eventuale documentazione allegata. Le operazioni sono inoltre siglate con marche temporali che "timbrano" in modo inequivocabile gli istanti di invio e ricezione.

Come garanti del servizio vengono costituiti dei **gestori accreditati** da parte del Centro Nazionale Informatica per la Pubblica Amministrazione (DigitPA). I gestori possono essere sia Enti Pubblici che soggetti privati.

Nel caso in cui il mittente smarrisca le ricevute, la traccia informatica delle operazioni svolte viene conservata dai gestori per un periodo di tempo definito, con lo stesso valore giuridico delle ricevute di risposta.

I messaggi possono includere testo, immagini, audio, video o qualsiasi altro tipo di file.

4.1 Specifiche Funzionali

Le specifiche tecnico-funzionali a cui qualsiasi sistema di PEC deve attenersi sono definite dal CNIPA nel documento "*Regole tecniche del servizio di trasmissione di documenti informatici mediante posta elettronica certificata*" e non sono quindi qui ripetute per brevità.

Lo schema logico di funzionamento è riassumibile nelle figure seguenti (tratte dal documento sopra citato) con associata la descrizione dei passi che rappresentano il flusso di funzionamento.

4.2 Busta di trasporto corretta e valida e consegna con esito positivo

Nel caso di funzionamento corretto con busta di trasporto corretta e consegna effettuata con esito positivo abbiamo il seguente flusso:

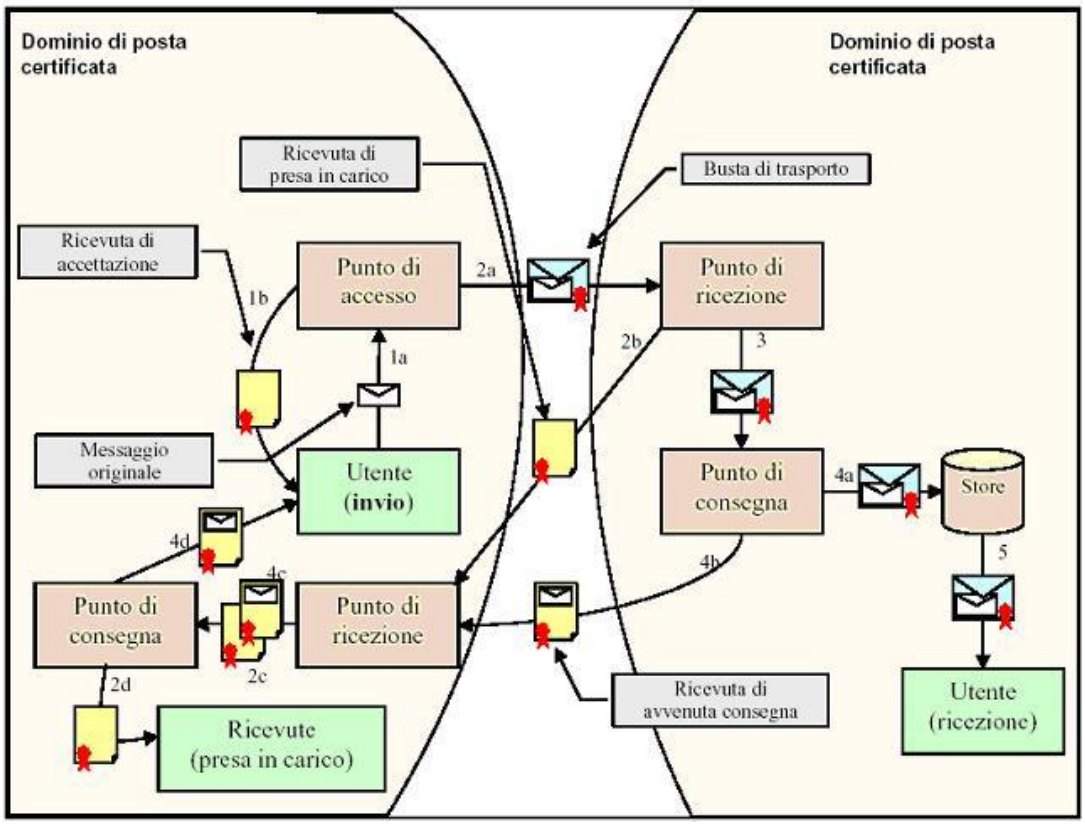


Figura 1 - Busta di trasporto corretta e valida con consegna avente esito positivo

- ✓ 1a – l'utente invia una e-mail al Punto di Accesso (PdA)
- ✓ 1b – il PdA restituisce al mittente una Ricevuta di Accettazione (RdA)
- ✓ 2a – il PdA crea una Busta di Trasporto (BdT) e la inoltra al Punto di Ricezione (PdR) del Gestore destinatario
- ✓ 2b – il PdR verifica la BdT e crea una Ricevuta di Presa in Carico (RdPiC) che viene inoltrata al PdR del Gestore mittente
- ✓ 2c – il PdR verifica la validità della RdPiC e la inoltra al PdC
- ✓ 2d – il PdC salva la RdPiC nello store delle ricevute del Gestore
- ✓ 3 – il PdR inoltra la BdT al Punto di Consegna (PdC)
- ✓ 4a – il PdC verifica il contenuto della BdT e la salva nello store (casella PEC del destinatario)
- ✓ 4b – il PdC crea una Ricevuta di Avvenuta Consegna (RdAC) e la inoltra al PdR del Gestore mittente
- ✓ 4c – il PdR verifica la validità della RdAC e la inoltra al PdC
- ✓ 4d – il PdC salva la RdAC nella casella PEC del mittente
- ✓ 5 – l'utente destinatario ha a disposizione la e-mail inviata

4.3 Busta di trasporto corretta e valida con errore di consegna

Nel caso di funzionamento corretto con busta di trasporto corretta ma con errore di consegna abbiamo il seguente flusso:

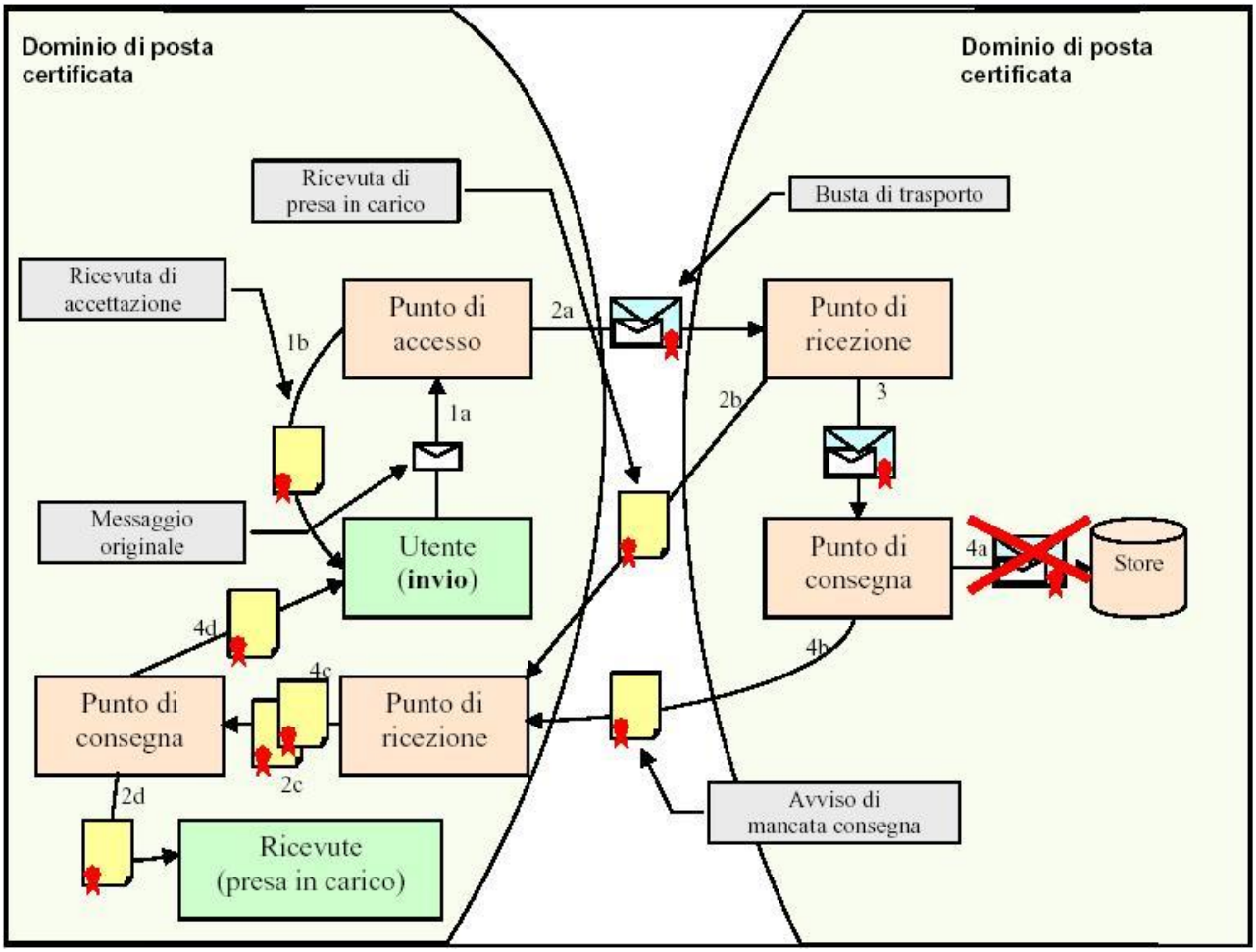


Figura 2 - Busta di trasporto corretta e valida con consegna avente errore di consegna

- ✓ 1a – l'utente invia una e-mail al Punto di Accesso (PdA)
- ✓ 1b – il PdA restituisce al mittente una Ricevuta di Accettazione (RdA)
- ✓ 2a – il PdA crea una Busta di Trasporto (BdT) e la inoltra al Punto di Ricezione (PdR) del Gestore destinatario
- ✓ 2b – il PdR verifica la BdT e crea una Ricevuta di Presa in Carico (RdPiC) che viene inoltrata al PdR del Gestore mittente

- ✓ 2c – il PdR verifica la validità della RdPiC e la inoltra al PdC
- ✓ 2d – il PdC salva la RdPiC nello store delle ricevute del Gestore
- ✓ 3 – il PdR inoltra la BdT al Punto di Consegna (PdC)
- ✓ 4a – il PdC verifica il contenuto della BdT ma non riesce a salvarla nello store (es. casella PEC del destinatario piena)
- ✓ 4b – il PdC crea un Avviso di Mancata Consegna (AMC) e la inoltra al PdR del Gestore mittente
- ✓ 4c – il PdR verifica la validità dello AMC e lo inoltra al PdC
- ✓ 4d – il PdC salva lo AMC nella casella PEC del mittente

4.4 Busta di trasporto contenente virus informatico non rilevato dal gestore mittente e consegna avente errore di consegna

Nel caso in cui il messaggio di trasporto contenga un virus non rilevato dal gestore mittente abbiamo il seguente flusso:

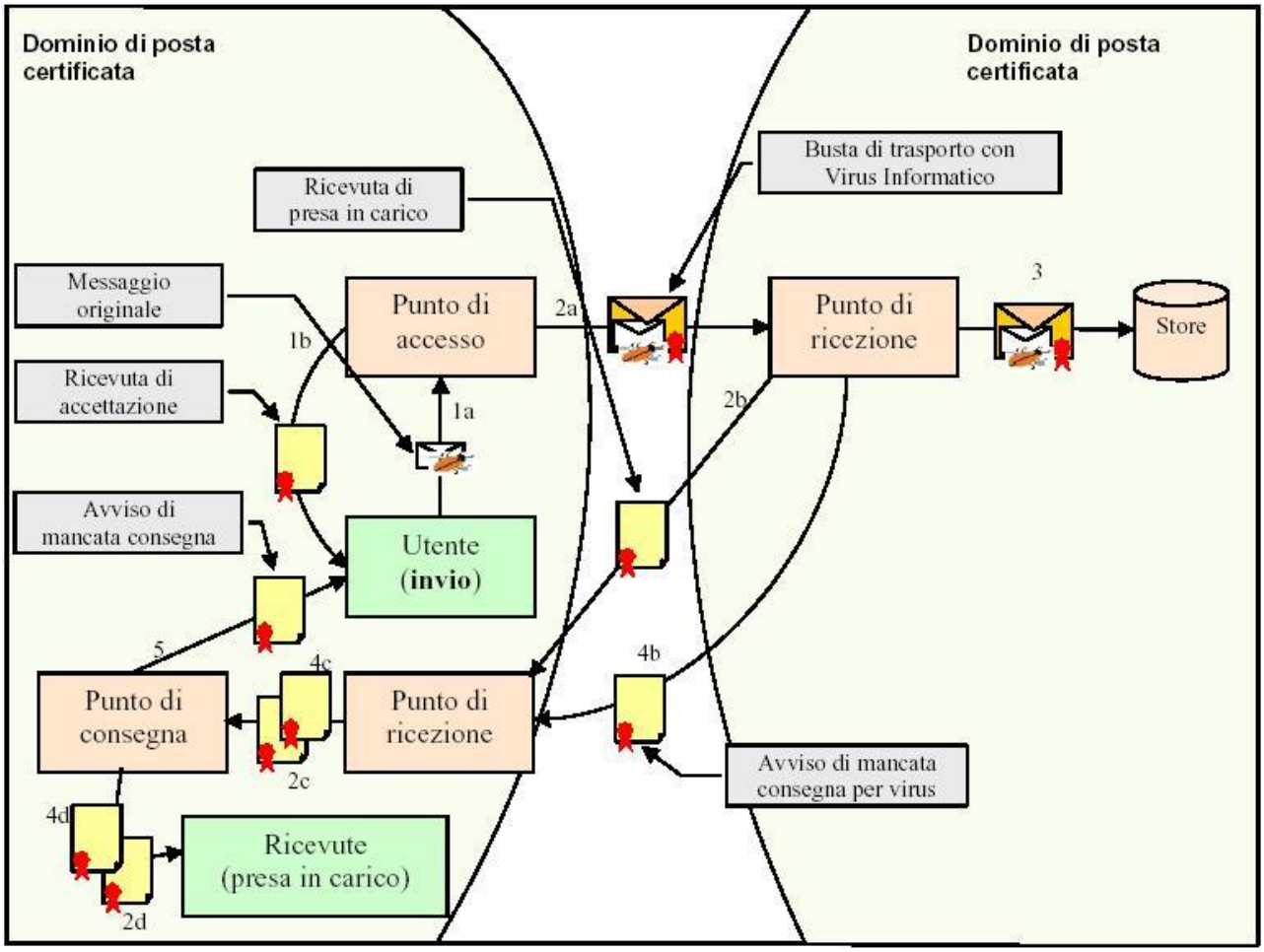


Figura 3 - Busta di trasporto corretta contenente virus informatico non rilevato dal gestore mittente e consegna avente errore di consegna

- ✓ 1a – l'utente invia una e-mail al Punto di Accesso (PdA)
- ✓ 1b – il PdA restituisce al mittente una Ricevuta di Accettazione (RdA)
- ✓ 2a – il PdA crea una Busta di Trasporto (BdT) e la inoltra al Punto di Ricezione (PdR) del Gestore destinatario
- ✓ 2b – il PdR verifica la BdT e crea una Ricevuta di Presa in Carico (RdPiC) che viene inoltrata al PdR del Gestore mittente
- ✓ 2c – il PdR verifica la validità della RdPiC e la inoltra al PdC
- ✓ 2d – il PdC salva la RdPiC nello store delle ricevute del Gestore
- ✓ 3 – il PdR verifica il contenuto della BdT, ne rileva un contenuto potenzialmente pericoloso e non la recapita al destinatario ma la conserva

- ✓ 4b – il PdR crea una Avviso di Mancata Consegna per Virus e la inoltra al PdR del Gestore mittente
- ✓ 4c – il PdR verifica la validità della RdAC e la inoltra al PdC
- ✓ 4d – il PdC salva l'Avviso di Mancata Consegna per Virus nello store delle ricevute del Gestore
- ✓ 5 – il PdC crea una Ricevuta di Mancata Consegna (RdE) e la inoltra nella casella PEC del mittente.

4.5 Messaggio originale con virus informatico rilevato dal gestore mittente

Nel caso in cui il messaggio originale contenga un virus e che tale virus venga rilevato dal gestore del mittente abbiamo il seguente flusso:

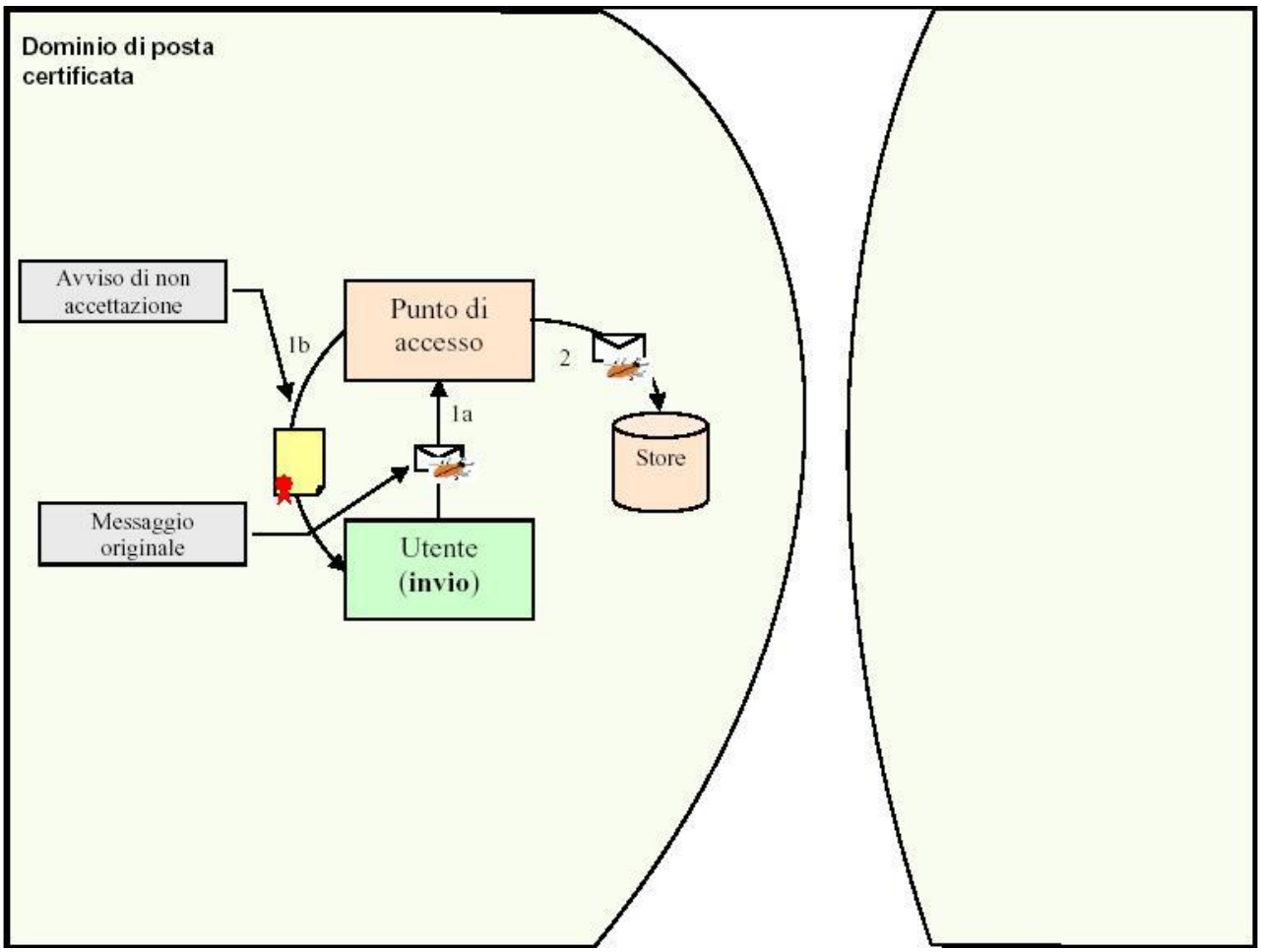


Figura 4 - Messaggio originale con virus informatico rilevato dal gestore mittente e avviso di non ac

- ✓ 1a – l'utente invia una e-mail al Punto di Accesso (PdA)
- ✓ 1b – il PdA rileva un contenuto potenzialmente pericoloso e restituisce al mittente una Avviso di non accettazione (ANA)
- ✓ 2 – il PdA non recapita al destinatario il messaggio ma lo conserva

4.5.1 Interazione tra un dominio convenzionale ed un dominio certificato

Nel caso in cui un utente appartenente ad un dominio non certificato invii una mail ad un utente di un dominio certificato, abbiamo il seguente flusso:

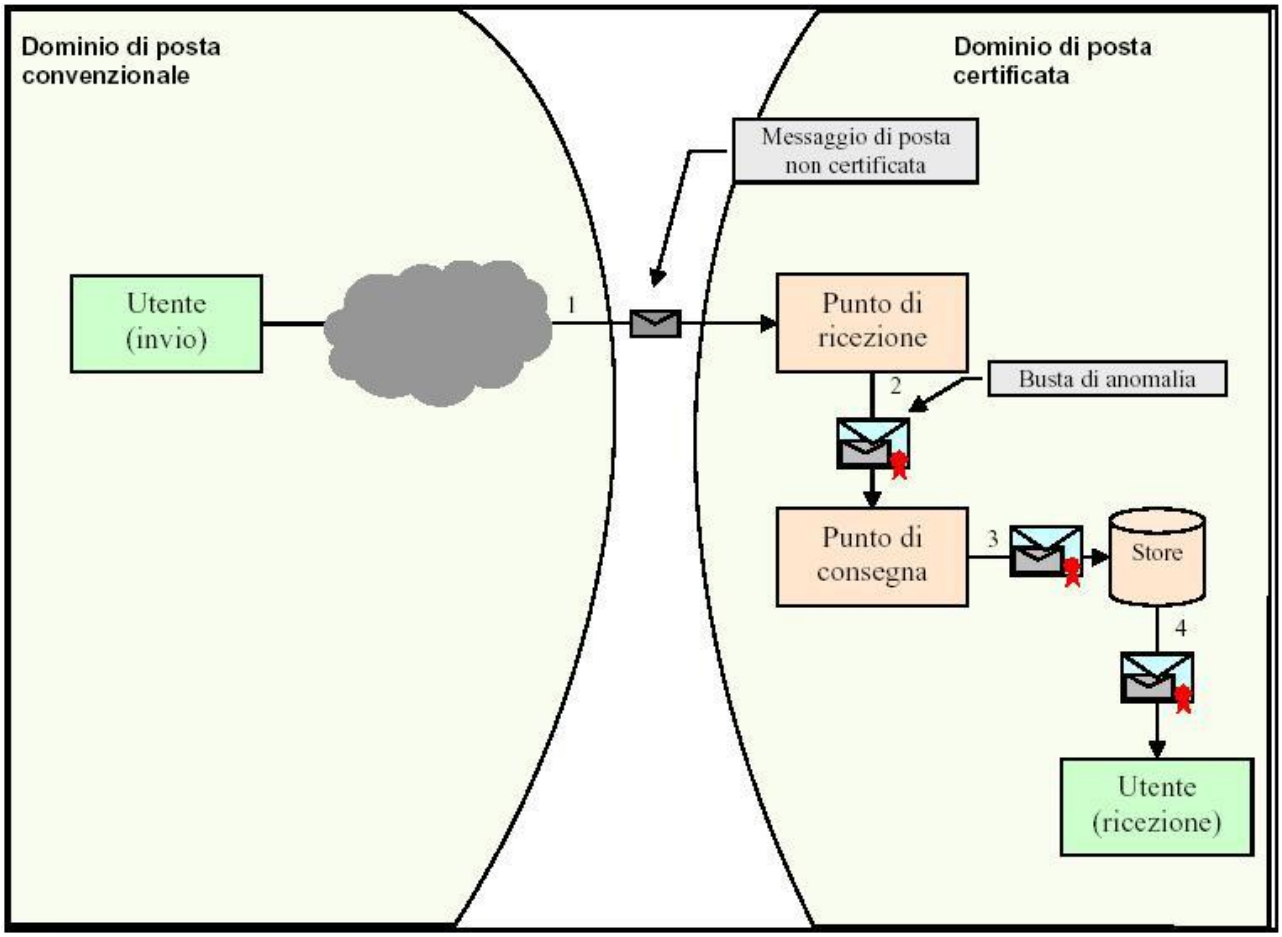


Figura 5 - Interazione fra un dominio di posta convenzionale (mittente) ed un dominio di posta certificata (ricevente)

- ✓ 1 – il messaggio n certificato viene inviato e raccolto dal PdR del Gestore Destinatario
- ✓ 2 – il PdR genera una busta di anomalia di trasporto e la invia al PdC
- ✓ 3 – il PdC consegna nella casella PEC dell'utente il messaggio
- ✓ 4 – l'utente destinatario ha a disposizione la e-mail inviata

Nel caso in cui un utente appartenente ad un dominio certificato invii una mail ad un utente di un dominio non certificato, abbiamo viceversa il seguente flusso:

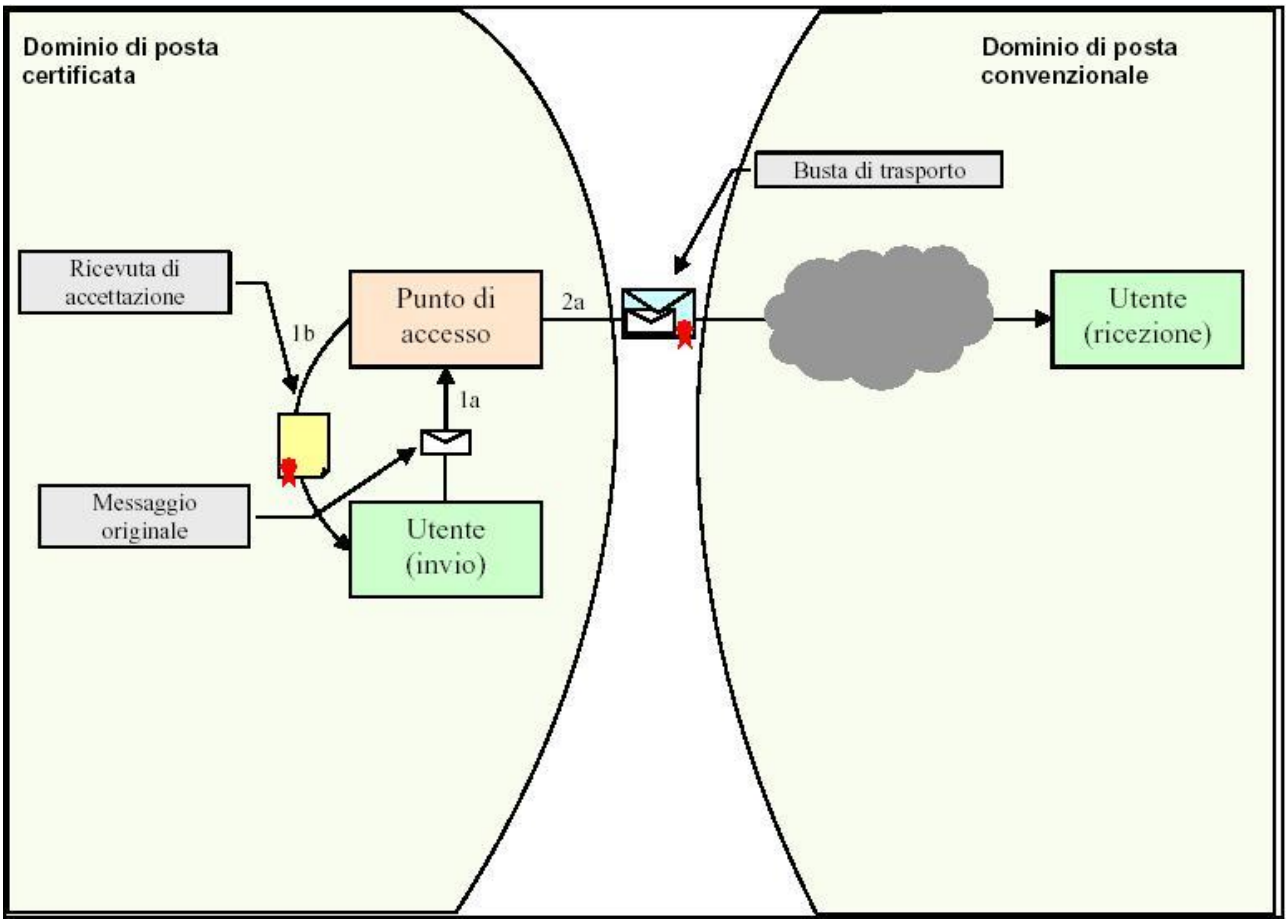


Figura 6 - Interazione fra un dominio di posta certificata (mittente) ed un dominio di posta convenzionale (ricevente)

- ✓ 1a – il Mittente invia il messaggio di posta elettronica certificata
- ✓ 1b – il PdA genera la ricevuta di accettazione e la invia all'utente
- ✓ 2a – il PdA genera la busta di trasporto e la invia al destinatario
- ✓ il destinatario riceve correttamente il messaggio imbustato all'interno del messaggio di trasporto

4.5.2 Specifiche del client di posta

Per quanto riguarda il sistema client, le specifiche tecnico funzionali che devono essere rispettate per poter garantire ad un utente di un generico sistema di posta certificata l'insieme minimo di funzionalità operative sono:

- ✓ gestione del colloquio con i punti di accesso e di consegna mediante l'utilizzo di canali sicuri;

- ✓ gestione dell'autenticazione dell'utente in fase di invio e di ricezione dei messaggi;
- ✓ supporto del formato MIME secondo RFC 2045 - RFC 2049;
- ✓ gestione del media type "message/rfc822";
- ✓ supporto del set di caratteri "ISO-8859-1 (Latin-1)";
- ✓ supporto dello standard S/MIME versione 3 come da RFC 2633 per la verifica delle firme delle buste e delle ricevute

4.5.3 Ricevuta di avvenuta consegna

Nell'istante in cui invia il proprio messaggio, l'utente ha la possibilità di decidere il tipo di ricevuta di avvenuta consegna che desidera ricevere tra completa (default), breve e sintetica:

- ✓ La **ricevuta completa** contiene, oltre ai dati di certificazione, il messaggio originale in allegato; con questa ricevuta il mittente può verificare che il messaggio consegnato sia effettivamente quello spedito.
- ✓ La **ricevuta breve** contiene, oltre ai dati di certificazione, gli hash crittografici (in allegato) del messaggio originale. Questo tipo di ricevuta è stata introdotta per ridurre le dimensioni dei messaggi trasmessi. Il mittente ha la possibilità di verificare che il messaggio consegnato sia effettivamente quello spedito a patto di conservare gli originali *inalterati* degli allegati al messaggio inviato.
- ✓ La **ricevuta sintetica** contiene i soli dati di certificazione ed è particolarmente utile per le trasmissioni automatiche che non necessitano di supervisione "umana".

5 – IL SERVIZIO PEC EROGATO

5.1 Target

La Regione Basilicata rivolge la propria offerta alle pubbliche amministrazioni ed ai privati, limitatamente ai rapporti intrattenuti tra le amministrazioni medesime ed i privati cui sono rilasciate le caselle di posta elettronica certificata.

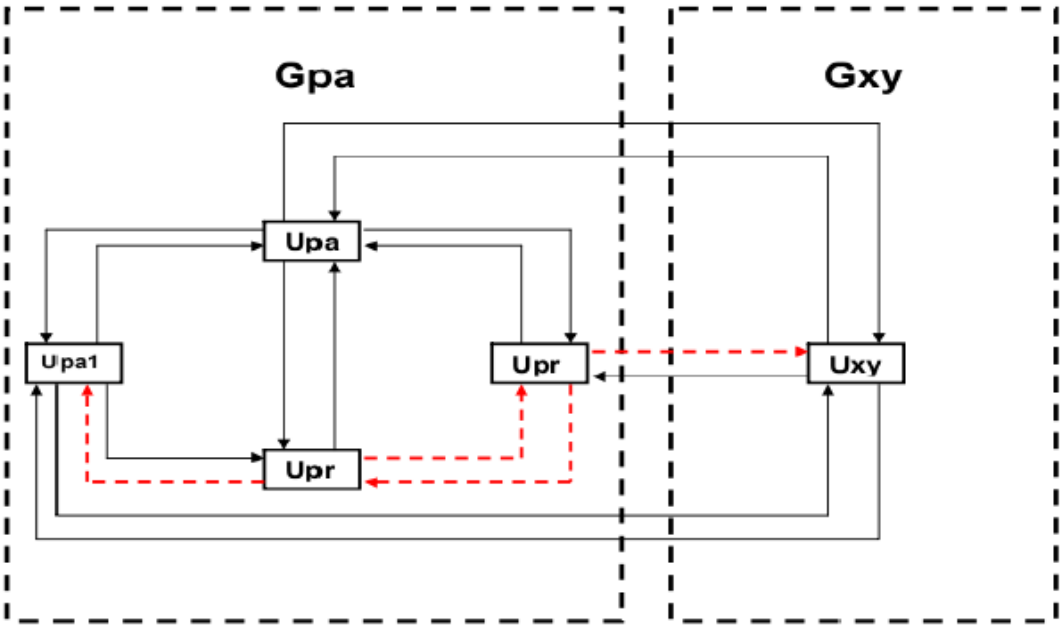
Il DPR 11 febbraio 2005, n.68 , art 16. comma 2 recita:

“L'utilizzo di caselle di posta elettronica certificata rilasciate a privati da pubbliche amministrazioni incluse nell'elenco di cui all'articolo 14, comma 2, costituisce invio valido ai sensi del presente decreto limitatamente ai rapporti intrattenuti tra le amministrazioni medesime ed i privati cui sono rilasciate le caselle di posta elettronica certificata.”

Pertanto lo scenario previsto nel comma 2 prevede: un Gestore di PEC che sia una PA (Gpa), degli utenti (Upa) che appartengono alla stessa PA e dei privati (Upr) che hanno in uso il servizio reso disponibile da Gpa.

Per completare il quadro, rendendolo coerente ad una possibile situazione reale, è opportuno considerare anche: gli utenti (Upa1), del servizio reso disponibile da Gpa, che facciano riferimento a delle PA distinte da quella del Gestore, un ulteriore generico Gestore di PEC (Gxy) e gli utenti di tale Gestore (Uxy).

Tale scenario può essere rappresentato graficamente come segue:



Le linee rosse tratteggiate evidenziano gli scambi di messaggi non ammessi dal comma 2.

Quindi, in sintesi, valgono le seguenti affermazioni:

1. Upr può ricevere da qualsiasi soggetto ma può inviare unicamente ad Upa;
2. Upa, Upa1 e Uxy possono scambiarsi, tra loro, messaggi senza vincoli.

Facendo riferimento a precedente schema interpretativo del comma 2, il sistema di PEC utilizzato dal generico Gestore Gpa deve essere in grado di fornire queste ulteriori specifiche funzionalità:

1. gestire almeno tre distinti insiemi di utenti: Upa, Upa1 e Upr;
2. nel caso in cui il mittente appartenga all'insieme Upr, il sistema deve produrre la ricevuta di accettazione solo se il destinatario appartiene all'insieme Upa altrimenti, per destinatari appartenenti agli insiemi Upa1 e Upr, produrrà un avviso di non accettazione

5.2 Tipologia di offerta

L'offerta riguarda ,

- ✓ la fornitura di caselle
- ✓ la fornitura di caselle associate ad un dominio esistente

5.2.1 Fornitura di caselle

- ✓ Il gestore offre la possibilità di richiedere caselle di PEC con le seguenti caratteristiche:
- ✓ indirizzo: nome.cognome@pec.basilicatanet.it
- ✓ dimensione iniziale: 1 Gb

Il nome della casella PEC viene proposto dal richiedente. Il Gestore del Servizio si riserva il diritto di rifiutare tale richiesta.

Alcune cause di tale rifiuto possono essere, a titolo esemplificativo ma non esaustivo, casi di omonimia, nomi troppo lunghi, nomi simili a marchi noti o afferenti ad Enti ed Istituzioni pubbliche diverse dal richiedente, ecc.

La dimensione della PEC può essere estesa su esplicita richiesta da parte del titolare.

5.2.2 Fornitura di caselle associate ad un dominio esistente

Il domino predefinito è pec.basilicatanet.it, ma per enti di particolare rilevanza in termini di dimensione ed importanza nell'ambito territoriale di riferimento è possibile utilizzare un proprio dominio registrato.

In tal caso la gestione del dominio è a carico dell'ente richiedente, il quale dà indicazioni al gestore del proprio dominio per la configurazione opportuna dei server DNS al fine di assicurare la visibilità in rete dei server coinvolti nel processo di trasmissione.

La responsabilità della corretta configurazione del DNS è esclusiva competenza del richiedente come previsto nella specifica contrattuale col gestore del dominio. I servizi relativi al dominio certificato vengono emessi dal Gestore del Servizio di Posta Certificata.

5.3 Accesso al servizio

Dal punto di vista dell'utente finale la casella PEC può essere vista come una comune casella di posta elettronica e come tale può essere acceduta attraverso i più diffusi client di posta ed attraverso un sistema di web mail.

5.3.1 Primo Accesso

Il titolare al primo accesso al pannello di gestione della posta elettronica certificata riceverà dal sistema la richiesta di modifica della password di primo accesso con una password personale, che risponda a precisi requisiti di sicurezza e che deve essere lunga almeno 8 caratteri e deve contenere almeno un numero ed una lettera maiuscola". Per tanto la prima pagina mostrata a seguito del login sarà quella dedicata al cambio password. Una volta effettuata la modifica della password, il titolare potrà accedere alle funzionalità previste.

5.3.2 Accesso attraverso i client di posta

Il sistema è compatibile con tutti i principali client di posta.

Per il corretto funzionamento è necessario che il client di posta venga abilitato a connettersi ai server pec attraverso i parametri di configurazione indicati nella tabella seguente:

SERVIZIO	*URL*	*PORTA TCP*
POP3/S	pop3.pec.basilicatanet.it	995
IMAP/S	imap.pec.basilicatanet.it	993
SMTP/S	smtp.pec.basilicatanet.it	465

Le istruzioni per la configurazione del client di accesso alla posta elettronica certificata saranno comunicate dal gestore al titolare della casella PEC nel messaggio di conferma attivazione.

L'utilizzo del sistema attraverso i client di posta è del tutto simile all'utilizzo nel caso di caselle di posta tradizionali. La sola differenza è di tipo funzionale: per ogni messaggio inviato il mittente riceve una ricevuta di accettazione e, se tutto va bene, una ricevuta di avvenuta consegna; il destinatario, dal canto suo, riceve il messaggio originale imbustato in un messaggio di trasporto il cui oggetto ha un prefisso del tipo “Posta Certificata:” seguito dal subject originale.

Sul sito del gestore vengono descritte le modalità di configurazione dei principali client di posta (Outlook, Thunderbird, Eudora, etc).

5.3.3 Accesso tramite web mail

Il Titolare potrà accedere alla casella di posta elettronica certificata, utilizzando un browser internet e collegandosi all'applicazione Webmail tramite il portale della PEC contattatile all'indirizzo http://pec.basilicatanet.it all'interno del quale è presente il collegamento alla webmail oppure direttamente all'url della webmail: https://webmail.pec.basilicatanet.it.

Se l’utente utilizza la posta elettronica certificata via browser (Webmail) non è necessaria alcuna configurazione.

E' possibile accedere al sistema di posta elettronica certificata inserendo le proprie credenziali che verr comunicato dal gestore nel messaggio di conferma attivazione.

Al sistema si accederà attraverso una interfaccia web, in modo trasparente per l’utente, perché l’autenticazione avverrà in SingleSignOn e le credenziali tra il sistema IMS e la “Web Mail” verranno passate in modo sicuro.

Una volta entrati nel sistema l'utente ha la possibilità di:

- ✓ consultare i messaggi arrivati
- ✓ inviare nuove mail
- ✓ ricercare i messaggi in base all'oggetto
- ✓ gestire la propria rubrica
- ✓ creare, modificare ed eliminare le cartelle
- ✓ modificare le impostazioni dell'applicazione.

Per ogni messaggio l'utente ha la possibilità di scegliere il tipo di ricevuta di avvenuta consegna che intende ottenere dal destinatario. La ricevuta, come detto al par. 4.5.3, può essere completa (contiene il messaggio originale), breve (contiene una codifica hash del messaggio originale) o sintetica (contiene i soli dati di certificazione).

5.4 Smarrimento di login e password di accesso

Se il cliente smarrisce la login o la password necessarie ad accedere al sistema può richiedere al Centro Servizi di inviargli nuovamente le credenziali via email. Questo avverrà dopo un'intervista telefonica con il titolare al quale verranno richieste informazioni quali:

- ✓ Nome e cognome o Ragione Sociale
- ✓ Indirizzo
- ✓ Città
- ✓ CAP
- ✓ Nazione
- ✓ Codice fiscale o partita IVA
- ✓ Verifica email

Il sistema offre comunque la possibilità di recuperare le credenziali di accesso tramite procedure online direttamente dalla pagina di autenticazione (https://ibasho.basilicatanet.it/ibasho_manager/enrolment/forgot_credential.faces).

5.5 Richiesta della cancellazione di una casella PEC da parte del titolare

Il titolare di una casella PEC può richiedere al proprio gestore di cancellare il proprio account. Per far questo il titolare deve inviare al gestore una richiesta contenente le seguenti informazioni:

- ✓ nome e cognome
- ✓ luogo e data di nascita
- ✓ indirizzo della casella PEC da eliminare
- ✓ fotocopia di un documento di identità

La richiesta può essere inviata:

- Via Fax: l'utente deve inviare al numero di fax 0971 471430 del centro servizi la richiesta compilata con le informazioni su indicate e firmata accompagnata alla fotocopia di un documento di identità (fronte-retro) valido del richiedente.

- Via eMail: l'utente deve inviare all'indirizzo mail del centro servizi, centroservizi@regione.basilicata.it, la richiesta compilata con le informazioni su indicate e firmata accompagnata alla fotocopia di un documento di identità (fronte-retro) valido del richiedente

Il gestore, dopo aver effettuato i dovuti controlli, provvederà alla eliminazione della casella PEC informando il titolare al termine dell'operazione.

5.6 Richiesta dei log dei messaggi da parte del titolare

Come previsto dalla normativa il titolare di una casella PEC può richiedere al proprio gestore un estratto dei log relativi ai messaggi da lui inviati o ricevuti. Il gestore, da parte sua, è obbligato a conservare tali log per un periodo minimo di 30 mesi.

Per richiedere un estratto dai log messaggi il titolare di una casella PEC deve effettuare esplicita richiesta inviando al gestore le seguenti informazioni:

- ✓ nome e cognome del titolare
- ✓ indirizzo PEC del mittente
- ✓ indirizzo PEC del destinatario
- ✓ data di riferimento del messaggio da ricercare
- ✓ oggetto del messaggio da ricercare (facoltativo)
- ✓ identificativo del messaggio (facoltativo)

La richiesta può essere inviata:

- Via Fax: l'utente deve inviare al numero di fax 0971 471430 del centro servizi la richiesta compilata con le informazioni su indicate e firmata accompagnata alla fotocopia di un documento di identità (fronte-retro) valido del richiedente.
- Via eMail: l'utente deve inviare all'indirizzo mail del centro servizi, centroservizi@regione.basilicata.it, la richiesta compilata con le informazioni su indicate e firmata accompagnata alla fotocopia di un documento di identità (fronte-retro) valido del richiedente

Dopo aver controllato che il documento di identità corrisponda effettivamente al titolare della casella PEC, verranno recuperate le informazioni e verrà inviato un messaggio di PEC al titolare contenente la tracciatura completa del messaggio. In particolare:

- ✓ data e ora ricevuta di accettazione
- ✓ data e ora ricevuta di presa in carico
- ✓ data e ora ricevuta di avvenuta consegna

Per ognuno di tali eventi verranno inviate al richiedente le seguenti informazioni:

- ✓ mittente del messaggio originale
- ✓ destinatari del messaggio originale
- ✓ oggetto del messaggio originale
- ✓ identificativo del messaggio originale
- ✓ data e ora dell'evento
- ✓ tipo di evento (accettazione, ricezione, consegna, emissione ricevute, errore, etc.)

5.7 Raccomandazioni per gli utenti

Per un utilizzo corretto del servizio riportiamo qui di seguito una lista di linee guida:

- ✓ Custodire con cura login e password di accesso al sistema.
- ✓ Utilizzare la casella PEC per le comunicazioni ufficiali e per gli usi consentiti dalla legge, evitando di usarla per le normali comunicazioni.
- ✓ Controllare frequentemente la casella di posta certificata in quanto i messaggi si intendono ricevuti nel momento in cui vengono depositati sulla casella PEC dell'utente indipendentemente dalla loro effettiva lettura.
- ✓ Cancellare i messaggi vecchi per evitare che la casella PEC raggiunga la massima capienza e non sia più possibile ricevere email.
- ✓ Proteggere il proprio computer con firewall e software antivirus.

5.8 Help desk

Per raccogliere le segnalazioni sulle funzionalità del sistema da parte degli utenti, è stato istituito un servizio di help desk attivo dal lunedì al venerdì, dalle ore 8:00 alle ore 20:00 ed il sabato dalle ore 8:00 alle ore 14:00, contattabile con le seguenti modalità:

- numero verde 800.29.20.20
- e-mail centroservizi@regione.basilicata.it
- fax 0971 471430

Il cliente potrà chiamare durante i suddetti orari per ottenere supporto sulle seguenti problematiche:

- ✓ informazioni generali sulla posta elettrica certificata e sul suo funzionamento
- ✓ validità legale dei messaggi di PEC

- ✓ interoperabilità con gli altri gestori
- ✓ uso della PEC nell'interazione con la pubblica amministrazione
- ✓ configurazione del client di posta
- ✓ funzionamento della web mail
- ✓ sicurezza ed affidabilità del sistema
- ✓ smarrimento delle credenziali di accesso al sistema (login, password)
- ✓ richiesta di invio del log messaggi
- ✓ problemi durante la connessione al server di PEC
- ✓ problemi durante l'invio e la ricezione di messaggi
- ✓ problemi di altra natura.

Le segnalazioni vengono registrate all'interno di un sistema di Help Desk che memorizza tutti i passaggi e le comunicazioni intercorse dall'apertura della chiamata (ticket) fino alla sua chiusura.

Il sistema, attraverso il tracciamento delle chiamate costruisce una knowledge base contenente le segnalazioni ed i problemi più frequenti, con le relative soluzioni. In questo modo l'operatore di help desk ha modo di individuare più velocemente la soluzione al problema segnalato.

5.9 Interoperabilità con gli altri sistemi di PEC

La Regione Basilicata si impegna a garantire l'interoperabilità del proprio servizio con gli altri gestori di PEC secondo quanto stabilito dalle Regole Tecniche di posta elettronica certificata (Decreto Ministeriale 2 novembre 2005). Per garantire l'interoperabilità la Regione Basilicata si impegna ad effettuare dei test di trasmissione con gli altri gestori accreditati presso il DigitPA.

5.10 Cessazione del servizio

Nel caso di cessazione dell'attività di gestore, la Regione Basilicata comunicherà questa intenzione al DigitPA con un anticipo di almeno 60 giorni, indicando, eventualmente, il Gestore o sostitutivo.

Con pari anticipo il Gestore informa della cessazione della attività tutti i possessori di caselle PEC da esso gestiti. Nella comunicazione, nel caso in cui non sia indicato un

gestore sostitutivo, sarà chiaramente specificato che tutte le caselle non saranno più accessibili dal momento della cessazione della attività del Gestore.

Regione Basilicata comunque prevede che le caselle oggetto di cessazione di servizio restino attive in sola lettura (senza possibilità di invio / ricezione messaggi) per un periodo non inferiore a 30 giorni a decorrere dal giorno definito per la cessazione del servizio.

5.11 Impegni del gestore

La Regione Basilicata in quanto Gestore di Posta Elettronica Certificata si impegna a:

- attenersi alle regole di cui al DM 2 novembre 2005 per l'accesso all'elenco pubblico dei gestori di Posta Elettronica Certificata;
- assicurare l'interoperabilità con gli altri gestori di Posta Elettronica Certificata;
- informare i Titolari sulle modalità di utilizzo del servizio e sui necessari requisiti tecnici;
- attenersi alle misure minime di sicurezza per il trattamento dei dati personali in conformità al D. Lgs 196/03;
- garantire il funzionamento regolare e sicuro del servizio;
- rilasciare al mittente che utilizza i propri servizi la ricevuta di accettazione nella quale sono contenuti i dati di certificazione che costituiscono prova dell'avvenuta spedizione del messaggio di Posta Elettronica Certificata;
- fornire al mittente le ricevute di avvenuta consegna;
- rilasciare, se Gestore della casella di Posta Certificata del destinatario, la ricevuta di presa in carico del messaggio al Gestore della casella del mittente;
- se Gestore mittente (nei casi di mancata ricezione, nelle 12 ore successive all'inoltro del messaggio, della ricevuta di presa in carico o di avvenuta consegna del messaggio inviato), comunicare al mittente che il Gestore del destinatario potrebbe non essere in grado di realizzare la consegna del messaggio e, in assenza di comunicazioni nelle successive 12 ore, comunicare al mittente l'avviso relativo alla mancata consegna del messaggio;
- comunicare al mittente, nei casi previsti e mediante un apposito avviso, la mancata consegna del messaggio;
- segnalare al destinatario i messaggi non qualificabili come Posta Elettronica Certificata;
- sottoscrivere con firma elettronica avanzata le ricevute rilasciate;

- sottoscrivere con firma elettronica avanzata le buste di trasporto, al fine di garantirne la provenienza, l'integrità e l'autenticità;
- apporre a ciascuna trasmissione un riferimento temporale generato con un sistema che garantisce uno scarto non superiore ad un minuto secondo rispetto alla scala di tempo universale coordinato (UTC), determinata ai sensi dell'art. 3, comma 1, della legge 11 agosto 1991, n. 273;
- trasmettere il messaggio di posta certificata, integro in tutte le sue parti, includendolo nella busta di trasporto;
- tenere traccia su appositi file di log di tutte le fasi di trasmissione e/o ricezione dei messaggi di posta certificata e conservare tali file per trenta mesi come previsto dalla vigente normativa;
- eseguire, senza soluzione di continuità, il salvataggio dei log dei messaggi generati nell'intervallo temporale predefinito;
- apporre giornalmente la marcatura temporale al file dei log relativo al periodo;
- trattare i virus secondo quanto previsto dal DM 2 novembre 2005, informando il mittente sul fatto che il messaggio inviato contiene un virus e conservando per 30 mesi i messaggi relativi;
- garantire i livelli di servizio previsti dal DM 2 novembre 2005.

6 – ARCHITETTURA

Questo capitolo descrive brevemente l'architettura di PEC utilizzata dalla Regione Basilicata.

La soluzione si basa sul prodotto OpenPEC, una soluzione open source per la Posta Elettronica Certificata.

6.1 OpenPEC : la storia del progetto

Il progetto OpenPEC nasce nell'agosto del 2003 con l'obiettivo di diventare il primo sistema Open Source di posta elettronica certificata conforme alle linee guida emesse dal Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA).

Il progetto viene iscritto su SourceForge.net (www.sourceforge.net), che rappresenta ormai il principale luogo di raccolta di materiale e progetti open source. Lo sviluppo del sistema avviene in forma collaborativa utilizzando le infrastrutture messe a disposizione da SourceForge.net.

Il progetto viene presentato al forum SALPA (Sapere Aperto e Libero nella Pubblica Amministrazione) tenuto a Pisa il 22 e 23 Marzo 2004 ed in occasione del convegno viene rilasciata la prima Beta Version.

Con il passare dei mesi si crea sempre più interesse sull'argomento e sul progetto e si costituisce una vivace community di collaboratori che forniscono il proprio contributo.

A Maggio del 2004 il team di sviluppo rilascia un'intervista alla rivista Linux Magazine che verrà poi pubblicata sul numero di Ottobre (n. 45).

Il progetto OpenPEC viene presentato alla Italian Perl Conference tenuta a Pisa il 22 e 23 Luglio 2004.

A luglio del 2004 termina lo sviluppo ed iniziano i test di interoperabilità da parte del CNIPA. I test si concludono brillantemente senza che vengano riscontrate non conformità ed il 2 agosto 2004 OpenPEC viene dichiarato conforme alle linee guida vigenti ed ufficialmente segnalato tra le soluzioni certificate.

A seguito della certificazione viene resa disponibile la release ufficiale 1.0.0 che viene rilasciata con licenza di utilizzo GNU General Public License.

Successivamente vengono rilasciate altre release che risolvono alcuni piccoli bug o ottimizzano il codice.

A seguito dell'uscita delle nuove regole tecniche a novembre 2005, iniziano le attività di sviluppo per adeguare OpenPEC alla nuova normativa.

Sviluppate le nuove funzionalità e dopo una significativa fase di test viene rilasciata la versione 2.0 di OpenPEC completamente aderente alla normativa vigente.

6.2 Vantaggi di una soluzione open source

Il software Open Source presenta una serie di vantaggi rispetto al software sottoposto a licenza proprietaria, in particolar modo per le pubbliche amministrazioni, in sintesi:

- ✓ Riduzione dei costi (non solo di licenza);
- ✓ Eliminazione del rischio di lock-in con software, protocolli e formati proprietari;
- ✓ Sicurezza (attacchi e trattamento dati);
- ✓ Maggiori opportunità per aziende locali;
- ✓ Favorisce naturalmente il riuso in ambito PA e quindi un miglior utilizzo del denaro pubblico.

Inoltre, l'utilizzo dei formati aperti assicura alcuni importanti benefici quali:

- ✓ *Indipendenza*: la documentazione pubblica e completa del formato consente l'indipendenza da uno specifico prodotto e fornitore;
- ✓ *Interoperabilità*: usando formati aperti sistemi eterogenei sono in grado di condividere gli stessi dati;
- ✓ *Neutralità*: I formati aperti non obbligano ad usare uno specifico prodotto, lasciando libero l'utente di scegliere sulla base del rapporto qualità/prezzo.

La soluzione basata su OpenPEC

OpenPEC non è un sistema di posta elettronica sviluppato completamente da zero ma si propone come estensione dei mail server Open Source più diffusi sul mercato e può essere visto come un "plug-in" di questi sistemi. Di seguito riportiamo uno schema che descrive i principali componenti della soluzione:

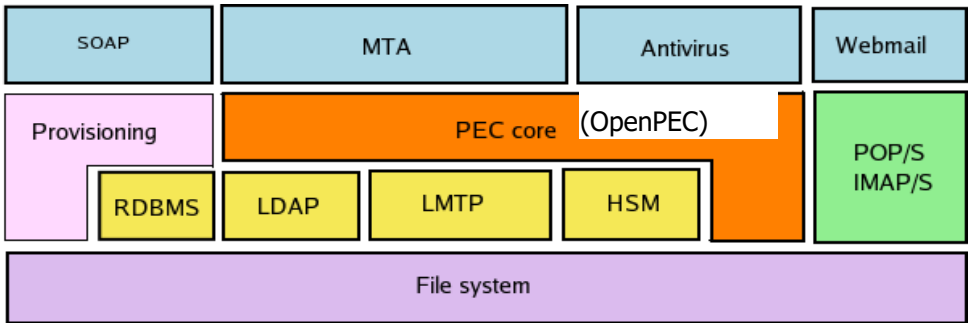


Figura 7 - Componenti del sistema

Come è possibile vedere dallo schema, esiste un nucleo centrale del sistema PEC core costituito da **OpenPEC** che si interfaccia con tutti gli altri moduli:

- ✓ il Mail Transfer Agent (**MTA**) che si incarica del "dispatching" delle mail;
- ✓ il modulo **Antivirus;**
- ✓ La componente **smtp/s**, per garantire l'accesso sicuro di un utente sul proprio mail server al momento di inviare un messaggio di posta;
- ✓ Le componenti **pop-s/imap-s/http-s** per l'accesso sicuro degli utenti alla propria casella PEC;
- ✓ Un server **LDAP** con la replica dell'indice centralizzato contenente l'elenco degli operatori PEC certificati. La replica, da effettuare con frequenza giornaliera, ha lo scopo di distribuire il carico, rendere il sistema ridondante ed evitare inutili colli di bottiglia;
- ✓ il database (**RDBMS**) che contiene gli account;
- ✓ il server **LMTP**;
- ✓ il modulo **HSM** utilizzato per la firma dei messaggi;
- ✓ lo storage (**file system)**;
- ✓ la **web mail;**
- ✓ il modulo di **provisioning** (per la creazione/modifica degli account) richiamabile attraverso interfaccia **SOAP.**

Le specifiche dettate dal DigitPA obbligano inoltre a mantenere un riferimento temporale con uno scarto non superiore ad 1 secondo rispetto al Tempo Universale Coordinato (UTC). Per questo motivo OpenPEC, attraverso il protocollo **NTP**, realizza la sincronizzazione temporale del sistema con l'Istituto Galileo Ferraris di Torino.

Sempre in base alle specifiche DigitPA, ogni soluzione di PEC deve conservare per un tempo stabilito i log che tracciano tutte le comunicazioni avvenute all'interno del sistema. Per garantirne l'integrità ed inalterabilità, i log vengono marcati temporalmente con un timestamp ottenuto da una **Time Stamping Authority** (**TSA**) riconosciuta. Per questo motivo OpenPEC contiene un'interfaccia, con protocollo standard, verso una TSA.

6.2.1 Storicizzazione dei Log e apposizione della marca temporale.

Al fine della conservazione dei log dei messaggi, di cui alle deliberazioni del CNIPA in materia di riproduzione e conservazione dei documenti su supporto ottico, è necessario definire un intervallo temporale unitario, non superiore alle ventiquattro ore, entro il quale eseguire senza soluzioni di continuità il salvataggio dei log dei messaggi generati in ciascun intervallo temporale.

Ai file generati da ciascuna operazione di salvataggio deve essere apposta la relativa marca temporale. Le marche temporali sono messaggi firmati digitalmente che legano in modo sicuro e verificabile un qualsiasi documento informatico ad un riferimento affidabile di tempo, data e ora. La validazione temporale di un documento informatico consiste nella generazione, da parte di una trusted third party (terza parte fidata), di una firma digitale così detta di *marcatura temporale* (time stamping), dalla quale è possibile acquisire la certezza della data ed ora di emissione. Le marche temporali possono risolvere dispute in merito al tempo (data/ora) in un cui un dato documento è stato prodotto.

Per il servizio di marcatura temporale è prevista l'integrazione di un servizio di Time Stamping Authority (TSA) esterno. A tale scopo OpenPEC è dotato di una interfaccia capace di interagire con una qualsiasi TSA secondo il protocollo standard RFC 3161 (http://www.ietf.org/rfc/rfc3161.txt) in modo da poter richiedere e ottenere la marca temporale relativa al log da storicizzare. I file generati possono così essere trasferiti su supporto ottico e conservati per il tempo stabilito dalla normativa (30 mesi).

6.2.2 Software antivirus

OpenPEC si interfaccia con i sistemi di antivirus tramite moduli software specifici per ogni tipo di antivirus: in fase di configurazione è possibile selezionare il modulo da caricare compatibile con il sistema antivirus presente e OpenPEC interagisce con il sistema in modo trasparente e compatibile con la normativa.

6.2.3 Conservazione dei messaggi contenenti virus e relativa informativa al mittente

OpenPEC, compatibilmente con la normativa, verifica la presenza dei virus nei messaggi di posta elettronica al Punto di Accesso, ossia nella fase immediatamente successiva alla

spedizione del messaggio originale, e al Punto di Ricezione, nella fase di ricezione dal sistema di posta certificato del mittente.

L'individuazione del virus fa scattare una serie di operazioni finalizzate ad avvertire il soggetto che ha introdotto il virus ed alla conservazione del messaggio per eventuali verifiche successive.

Se il virus è individuato al Punto di Accettazione verrà generato un “Avviso non accettazione per presenza di virus informatici” destinato al mittente del messaggio corrotto. Se invece il virus è rilevato al Punto di Ricezione verrà generato un “Avviso di rilevazione di virus informatici” destinato al gestore del sistema certificato del mittente e un “Avviso di mancata consegna per rilevazione di virus informatici” destinato al mittente del messaggio originale.

OpenPEC inoltre, conserva i messaggi contenenti virus su supporto di backup mettendo in condizioni il gestore di mantenerli per un periodo non inferiore a trenta mesi secondo quanto stabilito dalla normativa.

6.3 Architettura del sistema

Di seguito uno schema che descrive a grandi linee l'architettura del sistema di PEC della Regione Basilicata.

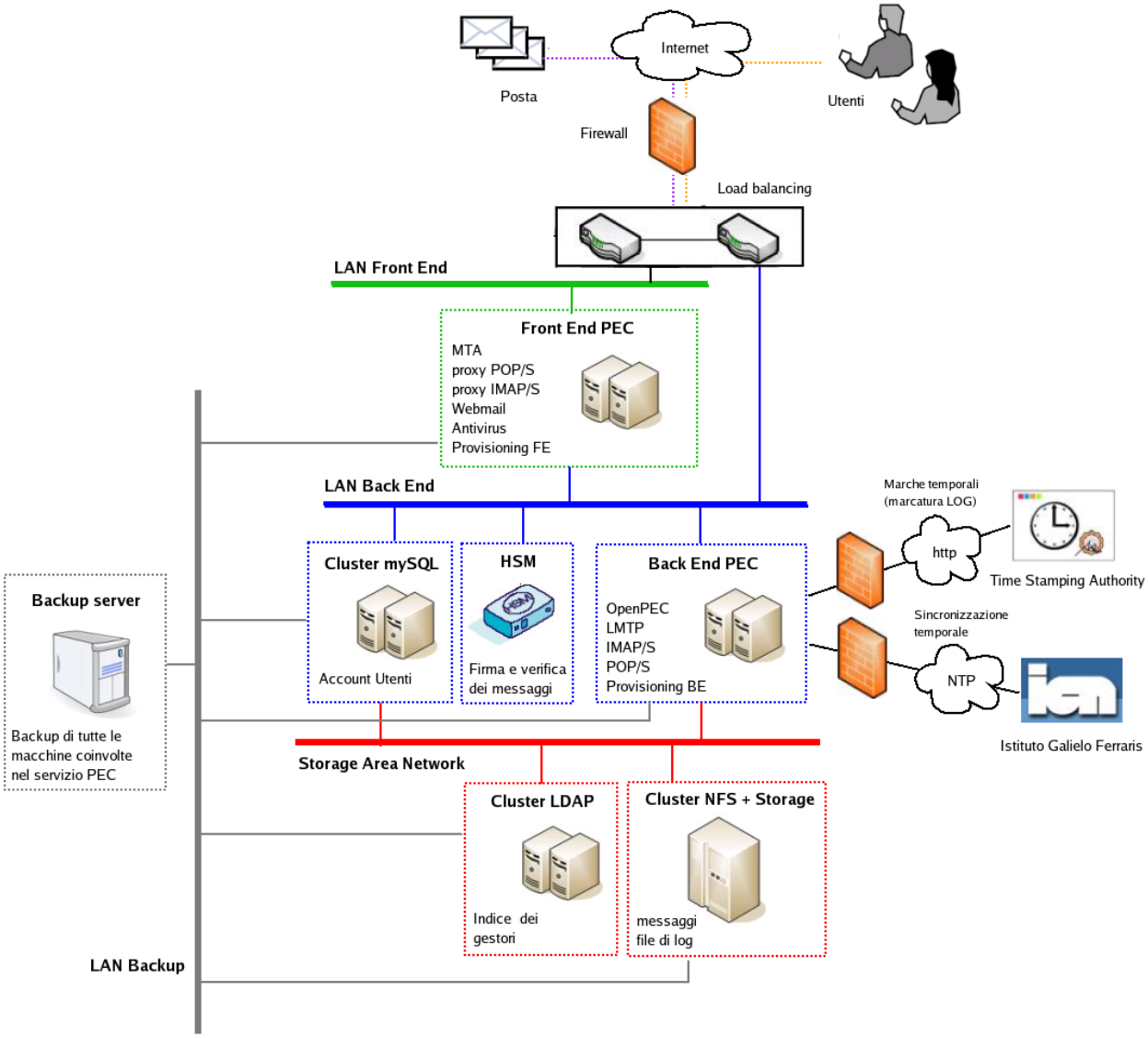


Figura 8 – Architettura del sistema

Come è possibile vedere dallo schema, il sistema è protetto da un modulo firewall e bilanciato dai moduli di load balancing. L'architettura applicativa è composta da un **Front End Layer**, un **Back End Layer** ed uno **Storage Layer**. E' inoltre presente una **LAN di**

Backup alla quale sono connesse tutte le macchine coinvolte nell'erogazione del servizio PEC.

Nel *Front End Layer* sono presenti

- ✓ i **server PEC di Front End** che contengono:
  - ○ i **server MTA** (Mail Transfer Agent) che si occupano dell'indirizzamento da e verso l'esterno dei messaggi
  - ○ il **proxy POP/S** che accetta le richieste di accesso POP/S da parte dell'utente e le gira verso il server POP contenuto nel livello di Back End
  - ○ la **web mail**
  - ○ il modulo **Antivirus**
  - ○ Il sistema di **Provisioning di Front End** che implementa le interfacce per la sottoscrizione e modifica degli account di PEC e si integra con il Provisioning di Back End.

Nel *Back End Layer* sono presenti:

- ✓ i **database server** che contengono gli account di PEC
- ✓ il modulo **HSM** per la firma e verifica dei messaggi
- ✓ i **server PEC di Back End** che contengono
  - ○ **OpenPEC** (nucleo centrale del sistema di PEC)
  - ○ il **server LMTP** che si incarica della consegna dei messaggi nelle caselle di PEC
  - ○ il **server POP/S** per l'accesso alle caselle con i clienti di posta da parte degli utenti
  - ○ il **server IMAP/S** per l'accesso alle caselle con i clienti di posta da parte degli utenti
  - ○ il modulo di **Provisioning di Back End** che implementa la sottoscrizione e la modifica degli account di PEC

  I server PEC si interfacciano inoltre con una Time Stamping Authority (TSA) per la marcatura temporale dei file di log e con l'Istituto Galileo Ferraris di Torino per la sincronizzazione dei clock attraverso il protocollo NTP (Network Time Protocol).

Nello *Storage Layer* sono presenti:

- ✓ i server **LDAP** (cluster) all'interno dei quali viene replicato l'indice pubblico dei gestori
- ✓ lo **storage** che contiene, su file system condiviso, i contenuti delle casella PEC degli utenti ed i file di log del sistema.

La *LAN di Backup* ha lo scopo di connettere con il **backup server** tutte le macchine coinvolte nel servizio di posta elettronica certificata sopra descritte. Il backup server si incarica di effettuare i salvataggi dei file di configurazione, i file di log, i dati e, in generale, tutte le informazioni critiche contenute nel sistema,

7 – CONDIZIONI DI FORNITURA

7.1 Dettagli offerta e condizioni di fornitura

La Regione Basilicata fornisce le caselle a titolo gratuito.

7.2 Livelli di servizio ed indicatori di qualità

Per l'erogazione del servizio la Regione Basilicata garantisce il rispetto dei livelli di servizio previsti dalla normativa.

Livelli di Servizio	
Numero massimo di destinatari contemporanei accettati	≥ 50
Dimensione massima di ogni singolo messaggio (intesa come prodotto tra il numero dei destinatari e la dimensione del messaggio)	≥ 100 MB
Disponibilità del servizio nel periodo di riferimento previsto (quadrimestre)	≥ 99,8%
Indisponibilità del servizio per il singolo fermo nel periodo di riferimento previsto (quadrimestre)	≤ 50%
Tempo massimo per il rilascio della ricevuta di accettazione nel periodo di disponibilità del servizio (calcolato escludendo i tempi di trasmissione)	30 min

Riportiamo qui di seguito gli indicatori di qualità del servizio (con giorni lavorativi si intendono i giorni dal lunedi al venerdi).

Indicatori di qualità	
Disponibilità del servizio (invio e ricezione email)	7 gg su 7 per 24 h
Disponibilità del servizio di richiesta di attivazione	7 gg su 7 per 24 h
Tempo per l'attivazione di un nuovo account di PEC (dalla ricezione di tutta la documentazione necessaria)	3 gg lavorativi

Indicatori di qualità	
Tempo massimo per l'esecuzione di interventi di manutenzione che causino il fermo servizio	2,8 h
Disponibilità del servizio di richiesta da parte del titolare della traccia delle comunicazioni effettuate (log)	7 gg su 7 per 24 h
Accesso ai file di log da parte del personale del Centro Servizi	dal lunedì al venerdì dalle ore 8 alle ore 14 e dalle 15 alle 18
Tempo massimo per l'invio delle informazioni relative ai file di log dietro richiesta del titolare	5 gg lavorativi
Sistema di monitoring con segnalazione dei malfunzionamenti e delle situazioni critiche rilevate	7 gg su 7 per 24 h
Assistenza standard tramite call center (trouble ticketing)	dal lunedì al venerdì dalle ore 8 alle ore 14 e dalle 15 alle 18

8 – STANDARD DI RIFERIMENTO, PROCEDURE DI SICUREZZA E OPERATIVE

8.1 Standard tecnologici

- RFC 1847 (Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted);
- RFC 1891 (SMTP Service Extension for Delivery Status Notifications);
- RFC 1912 (Common DContact Center NS Operational and Configuration Errors);
- RFC 2252 (Lightweight Directory Access Protocol (v3): Attribute Syntax Definitions);
- RFC 2315 (PKCS #7: Cryptographic Message Syntax Version 1.5);
- RFC 2633 (S/MIME Version 3 Message Specification);
- RFC 2660 (The Secure HyperText Transfer Protocol);
- RFC 2821 (Simple Mail Transfer Protocol);
- RFC 2822 (Internet Message Format);
- RFC 2849 (The LDAP Data Interchange Format (LDIF) – Technical Specification);
- RFC 3174 (US Secure Hash Algorithm 1 - SHA1);
- RFC 3207 (SMTP Service Extension for Secure SMTP over Transport Layer Security);
- RFC 3280 (Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List - CRL Profile).
- ISO/IEC 27002 come standard pratico di riferimento per le procedure di sicurezza.

8.1.1 Standard di sicurezza ISO/IEC 27002

Lo Standard **ISO/IEC 27002:2005** è una norma internazionale che fornisce i requisiti di un Sistema di Gestione della Sicurezza nelle tecnologie dell'informazione (Information Security Management System – ISMS). L'oggetto della norma è l'informazione, sotto qualsiasi forma e supporto, per la quale devono essere garantiti:

- ✓ La **riservatezza** (deve essere accessibile solo al personale autorizzato);
- ✓ L'**integrità** (deve essere mantenuta completa ed integra quando è necessario utilizzarla);
- ✓ La **disponibilità** (deve essere fruibile al personale autorizzato quando necessario).

Per garantire tutto ciò occorre anzitutto identificare i requisiti relativi alle informazioni gestite e valutarne i rischi associati in termini di:

- Conseguenze in caso di perdita delle informazioni o di inosservanza dei requisiti di riservatezza ad esse associati
- Probabilità che ciò accada
- Definizione delle azioni da intraprendere commisurate ai rischi
- Revisione periodica della valutazione del rischio.

La norma tratta in modo strutturato tutti i possibili aspetti legati alla sicurezza fisica, logica, ed organizzativa delle informazioni.

- ✓ **Sicurezza fisica**: il ruolo della sicurezza fisica è quello di proteggere:
  - le persone che operano nei siti ove si trovano le apparecchiature informatiche, dagli operatori agli utenti finali
  - le aree nelle quali si trovano i dispositivi informatici e di telecomunicazione, e le relative strutture ed impianti
  - i componenti del sistema informativo, inclusi i mezzi ed i sistemi di telecomunicazione
- ✓ **Sicurezza logica**: Il ruolo della sicurezza logica è quello di proteggere:
  - le informazioni trattate, quali documenti, archivi e banche dati
  - le reti e i protocolli di comunicazione
  - il software di base e di ambiente (incluso quello di controllo e gestione)
- ✓ **Sicurezza organizzativa** Il ruolo della sicurezza organizzativa è quello di garantire la continuità e l'efficacia dell'impegno del management. In altre parole:

- garantire l'efficacia del quadro organizzativo (poteri, responsabilità, compartimentazione, reporting e comunicazione, monitoraggio)
- garantire il rispetto di requisiti cogenti (leggi, norme, processi) e di standard interni
- diffondere la cultura della cooperazione e del controllo

In generale la norma rappresenta un ottimo punto di partenza per progettare un sistema di gestione della sicurezza delle informazioni, per quelle organizzazioni che necessitano di dotarsi di tale strumento per la criticità delle informazioni e dei dati gestiti. Sarà l'organizzazione stessa a dover valutare quali contromisure intraprendere a fronte di rischi identificati.

Il valore aggiunto di questa normativa è proprio nell'invito a considerare tutti gli aspetti legati alla sicurezza delle informazioni, anche quelli che la maggior parte delle organizzazioni non hanno mai valutato, ma che se si verificassero potrebbero creare notevoli danni all'organizzazione stessa, economici, legali e di immagine sul mercato.

8.1.2 Standard di riferimento per i dispositivi di firma

I device HSM utilizzati per la firma e verifica dei messaggi di PEC sono certificati **FIPS 2 – Level 3**. Con questa sigla si intendono i Requisiti Standard di Sicurezza (pubblicati dal NIST, il National Institute of Standards and Technology) che devono essere rispettati dai moduli crittografici utilizzati all'interno di un sistema di sicurezza ove si trattino dati/informazioni sensibili. In particolare fanno parte di questa gamma le specifiche dei moduli crittografici e relative interfacce, le regole, i servizi e il processo di autenticazione. Tra i requisiti, vengono trattati anche i vincoli di sicurezza a livello fisico ed il processo del Key Management.

Lo Standard si compone di quattro livelli qualitativi di sicurezza, dal Level 1 a 4 per coprire un'ampia gamma di requisiti, dal design all'implementazione dei moduli crittografici.

- ✓ Il **Level 1** riguarda essenzialmente i requisiti minimali di sicurezza per i moduli crittografici, in particolare per quanto riguarda gli algoritmi, senza alcun vincolo sulla sicurezza fisica.
- ✓ Il **Level 2** aggiunge, ai precedenti, requisiti fisici di sicurezza (ad es. è richiesto l'utilizzo di rivestimenti e/o etichette al fine di ottenere un livello fisico "tamper-evident").
- ✓ Il **Level 3** aggiunge, ai meccanismi di tamper-evidence presenti anche nei livelli precedenti altri meccanismi per garantire la tamper-proofness. I dispositivi, infatti, rispondono ai tentativi d'accesso non autorizzato cancellando la memoria del modulo crittografico. Inoltre, al meccanismo di autenticazione basato sui ruoli

previsto dal livello 2, il livello 3 aggiunge anche un meccanismo basato sull'identità: il modulo crittografico autentica l'identità di un operatore e verifica che sia associato ad un ruolo previsto e lo autorizza alla gestione di servizi specifici.

8.2 Gestione della sicurezza

L'obiettivo primario della gestione della sicurezza di un sistema informativo è quello di ridurre i rischi e di assicurare la continuità del servizio, prevenendo e minimizzando l'impatto degli eventuali incidenti.
La protezione di un sistema informativo richiede l'adozione di contromisure che possono essere sia di natura tecnica che non tecnica.

Il flusso logico applicato risulta quello in figura:

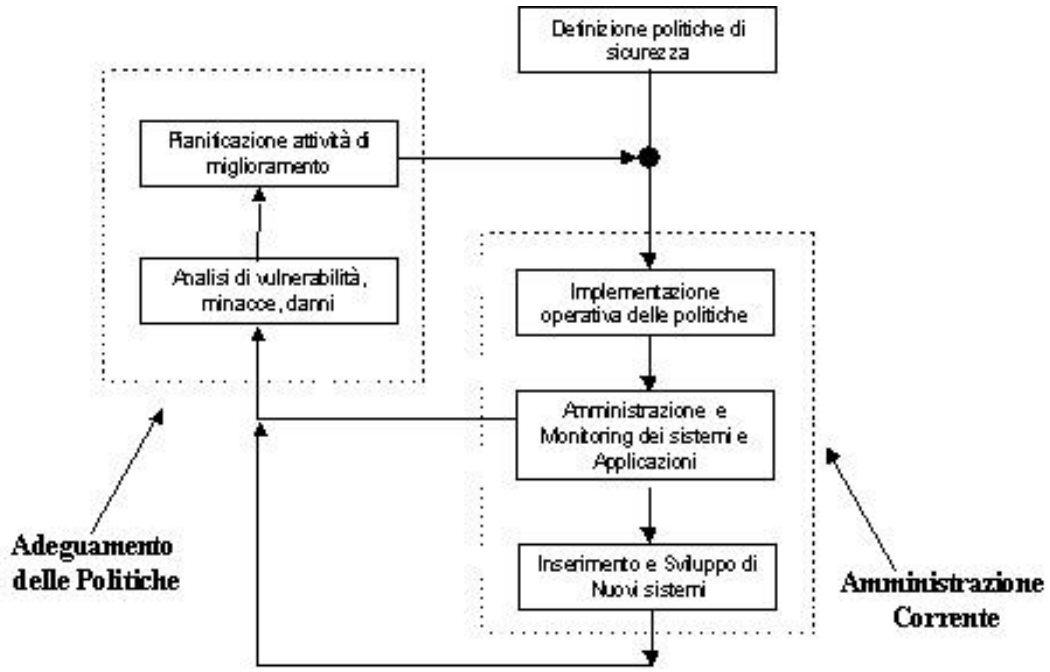


Figura 9 - Gestione della sicurezza: flusso logico

Esso prevede due momenti:

1. L'adeguamento delle politiche di Sicurezza generali.
2. L'amministrazione corrente della sicurezza che a sua volta presenta 2 casi:

- ✓ La gestione delle richieste degli utenti che, oltre alla attività di amministrazione quotidiana, comprende la **Gestione delle Richieste di Modifica** delle configurazioni del sistema di sicurezza ed il **Monitoraggio e Gestione delle performance.**
- ✓ Il **Monitoraggio e Gestione dei problemi/incidenti** finalizzata al monitoraggio, al mantenimento e all'implementazione di politiche di sicurezza definite, bloccando i tentativi di accesso fraudolento mediante l'uso di tutte le contromisure fino alla attivazione di una Unità di Crisi.

Per gestire gli aspetti di sicurezza dell'infrastruttura ICT del centro servizi, la Regione Basilicata effettua attività di:

- Monitoraggio delle componenti di sicurezza
- Gestione delle componenti di sicurezza
- Vulnerability Assessment

8.3 Misure di sicurezza

Il presente paragrafo descrive le misure di sicurezza adottate per:

- ✓ prevenire accessi fisici non autorizzati all'edificio ed ai locali che devono essere protetti;
- ✓ prevenire danni o interferenze nei locali ove si svolgono attività di trattamento dai dati personali;
- ✓ garantire e mantenere la sicurezza e l'integrità delle apparecchiature e degli impianti, al fine di evitare guasti che possono causare interruzione al funzionamento continuo delle attività.

Tali misure contrastano le minacce evidenziate nella Analisi dei Rischi relativa ai beni "Ambienti fisici".

8.3.1 Locali di erogazione del servizio

I locali nei quali sono situate le apparecchiature utilizzate per l'erogazione del servizio di PEC sono protetti da inferriate e serrande, porte blindate. E' inoltre presente un sistema anti-intrusione basato su telecamere perimetrali a circuito chiuso e rilevazione di movimento, collegato al servizio di vigilanza 24 ore su 24, per 7 giorni su 7.

I locali della server Farm sono protetti da pareti REI 180 e porta blindata REI 120 con chiave e codice numerico, l'accesso è concesso al solo personale addetto.

Nella server farm sono presenti impianti antincendio ed antifumo; i locali sono mantenuti ad una temperatura costante mediante un impianto di condizionamento.

I visitatori esterni possono accedere ai suddetti locali solo se accompagnati da personale interno autorizzato.

8.3.2 Infrastruttura tecnica

8.3.2.1 Sistema firewall

L'architettura di rete, articolata in più reti isolate per mezzo di una coppia di firewall, fornisce la possibilità di suddividere i sistemi del CTT in aree operative coerenti con la funzione dei sistemi stessi in modo da proteggerli opportunamente.

Sui firewall sono implementate opportune politiche di sicurezza che, agendo sulle porte TCP/IP e sui protocolli, filtreranno gli accessi tra le reti consentendo solo quelli previsti.

Le policy di sicurezza sono improntate alla filosofia che "*tutto quello che non é consentito è, di conseguenza, vietato*". Ciò implica che la maggior parte delle regole sono impostate per consentire il passaggio di traffico specifico mentre tutto il resto del traffico viene inglobato in poche regole di diniego.

8.3.2.2 Sistema Intrusion Detection System

Un'infrastruttura di rete non può ritenersi sicura soltanto con l'introduzione di un sistema firewall, ma deve necessariamente comprendere anche un sistema di "sorveglianza" delle intrusioni (**IDS** – **Intrusion Detection System**).

Il dispositivo di Intrusion Detection ha il compito di controllare la rete e di fornire alert, che siano facilmente rilevabili dal personale informatico addetto, su eventuali intrusioni o tentativi di intrusione al sistema.

La forza di un buon sistema di rilevamento delle intrusioni è soprattutto la sua capacità di segnalare tempestivamente, in modo efficace ed efficiente, gli eventi che possano essere rilevanti ai fini della sicurezza e nella integrazione dei dispositivi.

8.3.2.3 Apparati di connettività (routers e switch)

Gli apparati di interconnessione presenti nel CTT quali routers e switch presentano anch'essi delle caratteristiche e funzionalità di sicurezza. In particolare, i router implementano delle liste di controllo accessi ACL (Access Control List) che rappresentano una prima barriera di difesa contro gli attacchi provenienti da Internet.

L'utilizzo delle ACL sui router di frontiera può essere utile per effettuare un primo livello di filtro sui pacchetti provenienti da Internet, bloccando i pacchetti palesemente non coerenti con le politiche di sicurezza del Centro Servizi e consentendo quindi di coadiuvare il firewall nel proprio lavoro di filtro, sgravando quest'ultimo da un carico eccessivo di lavoro. In particolare, si può configurare il router per bloccare alcuni tipi di protocollo ritenuti intrinsecamente insicuri e quindi spesso non gestiti su segmenti esterni.

8.3.2.4 Sistema di Back-Up

Il sistema di backup svolge un ruolo fondamentale nel sistema complessivo della sicurezza e, più precisamente, nel sistema di Disaster Recovery. In caso di un evento 'disastroso', che provochi la distruzione di un supporto magnetico o un sistema hardware, è fondamentale la presenza di un backup affidabile che consenta il ripristino della situazione ad una certa data. Il sistema di backup, grazie alla sua architettura modulare, è scalabile ed è in grado di gestire sistemi distribuiti complessi.

Tramite il sistema di backup verranno programmate le operazioni di backup automatico periodico in modo da avere sempre a disposizione una copia recente delle informazioni importanti del CTT.

Tutto il sistema di backup opera principalmente su una rete LAN dedicata (BACKUP). Il server di backup è collegato sia a questa rete e sia alla LAN di Back End. Tutti i sistemi server sono collegati a tale rete mediante una interfaccia apposita.

8.3.2.5 I Dispositivi di firma dei messaggi

Il sistema garantisce un elevato grado di sicurezza soprattutto riguardo alla gestione delle chiavi private e dei certificati utilizzati per la generazione delle firme delle ricevute, degli avvisi e delle buste di trasporto e per il processo di verifica delle suddette operazioni.

Come HSM vengono utilizzati i prodotti di **nCipher** (www.ncipher.com), il più autorevole produttore a livello mondiale di prodotti e sistemi crittografici.

In particolare viene utilizzato il prodotto **netHSM™ 500**, un modulo hardware ad elevata sicurezza che, collegato in rete, costituisce una risorsa crittografica condivisibile per server multipli.

Figura 10 - netHSM 500 nCipher

8.3.3 Struttura organizzativa

8.3.3.1 Personale interno

Tutto il personale che svolge attività inerente la posta elettronica certificata viene formato internamente e possiede gli skill e l'esperienza necessari ad operare sul sistema.

Il personale viene responsabilizzato sulla criticità del servizio e viene stimolato a svolgere i compiti assegnati con la massima attenzione e precisione possibile.

Ogni risorsa dipende direttamente da uno dei responsabili del servizio (registrazione titolari, servizi tecnici, verifiche ed ispezioni, sicurezza) dal quale viene costantemente seguito e controllato.

8.3.3.2 Analisi e gestione dei rischi

Sono previste delle attività periodiche di analisi dei rischi nella quali i responsabili del servizio analizzano le criticità del sistema allo scopo di prevenire malfunzionamenti ed interruzioni del servizio. I possibili guasti vengono suddivisi in:

- ✓ guasti di normale entità (malfunzionamenti sui componenti software ed hardware) che, generalmente, non sono fonte di danni e non portano ad interruzioni del servizio e
- ✓ guasti di grande rilevanza (incendi, terremoti ed altri eventi catastrofici, atti dolosi, etc) che, viceversa, possono causare problemi seri all'intero sistema fino a provocarne l'interruzione.

Dopo aver analizzato nel dettaglio tutte le criticità, vengono individuae le misure preventive e risolutive per ogni tipo di guasto.

8.3.3.3 Controllo dei livelli di sicurezza

Il responsabile della sicurezza controlla costantemente l'intero sistema e verifica che i livelli previsti siano rispettati e non siano presenti criticità.

E' inoltre prevista almeno una visita ispettiva interna annuale durante la quale vengono analizzati i componenti del sistema (apparati di rete, server, device di firma, etc) e le risorse umane adibite all'erogazione del servizio allo scopo di individuare eventuali vulnerabilità.

In particolare i responsabili del servizio relazionano sull'operato del personale allo scopo di rimuovere tempestivamente le risorse giudicate non idonee o “a rischio”.

Il risultato della visita è un rapporto che descrive la situazione del sistema, le verifiche effettuate e l'elenco degli interventi da svolgere per migliorare il sistema.

8.3.4 Protezione dei dati

I dati personali degli utenti sono trattati, conservati e protetti dalla Regione Basilicata conformemente da quanto previsto dal Decreto legislativo n. 196 del 30 giugno 2003 “Codice in materia di protezione dei dati personali” (per i dettagli si rimanda al Cap. 10 −). Adottando le misure, le procedure, i processi ed i controlli di sicurezza descritti nei precedenti paragrafi, Regione Basilicata è in grado di assicurare, ai propri clienti, un continuo e costante livello di protezione dei propri dati.

8.4 Procedure operative

Per l'erogazione del servizio di posta elettronica certificata la Regione Basilicata mette in atto una serie di procedure tecniche ed organizzative che hanno l'obiettivo di garantire un livello di servizio elevato e costante nel tempo.

8.4.1 Organizzazione del personale

Come previsto dal DM del 2 novembre 2005, per l'erogazione del servizio sono state definite le seguenti figure professionali:

- ✓ 1 responsabile della registrazione dei titolari
- ✓ 1 responsabile dei servizi tecnici
- ✓ 1 responsabile delle verifiche e delle ispezioni (auditing)
- ✓ 1 responsabile della sicurezza, dei log dei messaggi e del sistema di riferimento temporale

I suddetti responsabili di settore possiedono l'esperienza necessaria secondo quanto specificato nel Decreto ministeriale del 2 novembre 2005.

A supporto di queste figure può essere affiancato, in base alle esigenze, personale specializzato in grado di svolgere le singole attività legate all'erogazione del servizio PEC.

Il suddetto personale possiede l'esperienza e le conoscenze necessarie a svolgere i compiti assegnati dai responsabili di settore e viene preventivamente ed opportunamente istruito attraverso appositi corsi di formazione interna.

8.4.2 Gestione backup

I sistemi sono soggetti a regolare backup dei file system su apparati a nastro utilizzati in modo condiviso dalle diverse applicazioni e servizi presenti all’interno della Server Farm

Il sistema e’ dotato delle più moderne infrastrutture per il salvataggio dei contenuti dei dischi. Il prodotto utilizzato controlla e gestisce l’esecuzione dei salvataggi e la loro archiviazione.

I backup dei dati, per gli eventuali ripristini in caso di guasto e per tutti gli altri casi previsti dalla normativa vigente, sono eseguiti giornalmente e settimanalmente secondo un sistema automatico e pianificato.

I backup giornalieri vengono effettuati su supporto magnetico in forma incrementale, mentre i backup settimanali sono di tipo full.

In aggiunta al sistema di salvataggio pianificato in maniera automatica, viene eseguito un ulteriore backup manuale di tipo full con cadenza mensile.

I nastri contenenti le copie di backup vengono conservati in cassaforte ignifuga, posta in un locale separato e distante alcuni chilometri dalla server farm di erogazione del servizio, dotato di sistemi di rilevamento anti-intrusione e presidio con agenti di vigilanza 24hx7x365.

8.4.3 Monitoring del sistema

Tutti i servizi utilizzati all'interno della soluzione PEC, siano essi hardware o software, vengono costantemente supervisionati attraverso un'applicazione di monitor. Per ogni servizio vengono definiti, a seconda dei casi, dei valori di soglia o dei trigger che servono a stabilire quando il sistema si trova in una situazione critica che può dare origine a malfunzionamenti. Al superare dei valori di soglia, o allo scattare dei trigger, il sistema di monitor segnala, via email, lo specifico malfunzionamento che è stato rilevato.

I segnali di alert vengono raccolti 24 ore su 24 dal team di Help Desk.

8.4.4 Gestione e risoluzione dei problemi

Riportiamo qui di seguito il flusso di gestione delle segnalazioni:

1. L'utente (il cliente) apre la segnalazione via telefono o via email
2. Nel caso di segnalazione telefonica, se l'operatore di help desk che prende in carico la chiamata è in grado di rispondere immediatamente nel corso della telefonata può decidere di non aprire un nuovo ticket a meno che non reputi la segnalazione e la risoluzione interessante ed utile (per usi futuri). Nel caso di segnalazioni non risolvibili immediatamente, l'operatore apre il nuovo ticket sul sistema di Help Desk.
3. Nel caso di segnalazioni via email, l'operatore apre un nuovo ticket sul sistema di Help Desk
4. All'apertura del ticket viene assegnato un identificativo univoco alla chiamata, identificativo che sarà utilizzato nel seguito per tutte le interazioni/comunicazioni con l'utente.
5. L'operatore può in qualsiasi momento aggiungere commenti e modificare il ticket (ad esempio nel caso di problemi imputabili a terzi può inserire i solleciti effettuati).

6. Nal caso in cui l'operatore non sia in grado di risolvere da solo il problema, può chiedere l'intervento di personale interno o esterno all'azienda. In tutti i casi rimarrà sempre lui il responsabile del ticket.
7. Nel caso di segnalazioni particolarmente gravi o al presentarsi di situazioni critiche l'operatore può decidere di far "scalare" il problema informando il responsabile del servizio di Help Desk
8. Se lo ritiene opportuno il responsabile del servizio di Help Desk può decidere di informare i responsabili di servizio che possono essere interessati al problema tra:
   - ✓ il responsabile del servizio PEC
   - ✓ il responsabile della registrazione dei titolari
   - ✓ il responsabile della sicurezza, dei log messaggi e del riferimento temporale
   - ✓ il responsabile dei servizi tecnici
   - ✓ il responsabile delle attività di auditing
9. Nel caso in cui per la risoluzione del problema sia necessario prevedere un'attività di manutenzione straordinaria, i sopra elencati responsabili dei servizi pianificano i tempi e le date degli interventi.
10. Nel caso in cui l'intervento di manutenzione straordinaria causi un fermo o una disfunzione del servizio, i responsabili di cui sopra ne comunicano data ed orario al customer care che informa a sua volta gli utenti finali.
11. Una volta terminato l'intervento, il customer care comunica agli utenti finali il completamento dell'attività di manutenzione straordinaria.
12. Risolto il problema, l'operatore di Help Desk effettua la chiusura del ticket ed informa l'utente che ha effettuato la segnalazione.

9 – OBBLIGHI E RESPONSABILITÀ

9.1 Obblighi e responsabilità del gestore

Il gestore di PEC ha l'obbligo di erogare il servizio di posta elettronica certificata nel rispetto della normativa vigente e delle Regole Tecniche contenute nel Decreto Ministeriale 2 novembre 2005. In particolare il gestore ha il dovere di garantire i livelli di servizio previsti, assicurare l'interoperabilità con gli altri gestori accreditati, conservare e rendere disponibili i file di log relativi alle trasmissioni avvenute nei domini da lui gestiti per gli usi e nelle modalità previste dalla legge.

La Regione Basilicata non assume alcun obbligo riguardo la conservazione dei messaggi inviati e trasmessi attraverso le proprie caselle di PEC. Il responsabile della conservazione dei messaggi è il cliente del servizio (titolare o utilizzatore).

La Regione Basilicata ha la responsabilità di mantenere il servizio di PEC conforme con la normativa vigente, adeguandolo nel caso di future disposizioni che saranno emanate.

La Regione Basilicata si riserva la facoltà di modificare il presente manuale nel caso in cui vengano apportate modifiche tecniche al sistema, variazioni all'offerta commerciale, o adeguamenti normativi.

La Regione Basilicata non ha alcuna responsabilità sui danni causati dall'uso improprio del servizio da parte dei propri clienti.

La Regione Basilicata non ha alcuna responsabilità sui contenuti dei messaggi inviati e ricevuti attraverso le proprie caselle di PEC, ancorchè illeciti o lesivi della morale e dell'ordine pubblico.

9.2 Obblighi e responsabilità del titolare

Il titolare del servizio ha l'obbligo di:

- ✓ fornire alla Regione Basilicata tutte le informazioni necessarie ad identificare la persona ed attivare il servizio, garantendo, sotto la propria responsabilità, la veridicità dei dati comunicati;
- ✓ custodire gelosamente le proprie credenziali di accesso al sistema;
- ✓ utilizzare in modo sicuro il sistema e non rivelare ad alcuno le proprie credenziali di accesso;
- ✓ utilizzare il servizio per i soli usi consentiti dalla legge;
- ✓ non cedere a terzi il servizio senza l'autorizzazione da parte della Regione Basilicata;

- ✓ essere a conoscenza dei contenuti del presente Manuale Operativo.

Il titolare ha la piena responsabilità del contenuto dei messaggi inviati e relativi allegati.

Il titolare ha la responsabilità di conservare copia dei messaggi inviati o spediti e relative ricevute.

9.3 Limitazioni ed indennizzi

La Regione Basilicata non risponderà in alcun caso dei danni causati direttamente o indirettamente dagli utilizzatori del servizio imputabili ad un utilizzo improprio del sistema ed al mancato rispetto delle regole e degli obblighi contenuti nel presente manuale.

Il gestore non potrà in alcun modo essere ritenuto responsabile di danni derivanti da cause di forza maggiore, caso fortuito, atti della Pubblica Autorità, eventi catastrofici (incendi, terremoti, esplosioni) o comunque non imputabili alla Regione Basilicata.

10 – PROTEZIONE DEI DATI PERSONALI

I presente capitolo del manuale operativo ha lo scopo di illustrare le procedure e le modalità operative adottate dal gestore per il trattamento dei dati personali, nello svolgimento della propria attività di gestore di PEC.

I dati personali relativi al richiedente la registrazione, al titolare di certificati, al terzo interessato e a chiunque acceda al servizio, sono trattati, conservati e protetti dalla Regione Basilicata conformemente da quanto previsto dal DECRETO LEGISLATIVO 30 giugno 2003, n.196 recante il "Codice in materia di protezione dei dati personali" (in S.O n. 123 alla G.U. 29 luglio 2003, n. 174) integrato con le modifiche introdotte dal DECRETO LEGISLATIVO 10 agosto 2018, n. 101, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonchè alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)" (in G.U. 4 settembre 2018 n.205).

Ai sensi dell'art. 13 del Regolamento Generale Europeo per la protezione dei dati personali (GDPR) General Data Protection Regulation (UE) 2016/679, la Regione Basilicata, in qualità di "Titolare" del trattamento, fornise informazioni in merito all'utilizzo dei dati personali degli utenti posta elettronica certificata.

10.1 Fonte dei dati personali

La raccolta dei dati personali viene effettuata registrando i dati forniti dagli utenti, in qualità di interessati, al momento della compilazione della modulistica per la presentazione dell'istanza per il rilascio dell'account di rete e/o posta elettronica della Regione Basilicata.

In particolare, i dati trattati sono: i dati anagrafici, foto documento d'identità e Codice Fiscale.

10.2 Finalità del trattamento e base giuridica

I dati personali sono trattati esclusivamente per il rilascio delle credenziali di accesso alla Posta Elettronica Certificata della Regione Basilicata

Il fine è l'utilizzo dei servizi telematici

La base giuridica è il Codice dell'Amministrazione Digitale D.lgs 82/2005.

10.3 Modalità di trattamento dei dati

In relazione alle finalità descritte, il trattamento dei dati personali avviene mediante strumenti mnuali, informatici e telematici con logiche strettamente correlate alle finalità sopra evidenziate e, comunque, in modo da garantire la sicurezza e la riservatezza dei dati stessi in conformità alle disposizioni previste dall'articolo 32 GDPR.

10.4 Facoltatività del conferimento dei dati

Il conferimento dei dati è facoltativo, ma in mancanza non sarà possibile adempiere alle finalità descritte al punto "Finalità del trattamento".

10.5 Categorie di soggetti ai quali i dati possono essere comunicati o che possono venirne a conoscenza in qualità di Responsabili o Incaricati

I dati personali degli utenti potranno essere conosciuti esclusivamente dai funzionari della Regione Basilicata individuati quali autorizzati e/o Incaricati del trattamento. Esclusivamente per le finalità previste al punto "Finalità del trattamento", possono venire a conoscenza dei dati personali società terze fornitrici di servizi per la Regione Basilicata, previa designazione in qualità di Responsabili esterni del trattamento e garantendo il medesimo livello di protezione. Alcuni dati personali comunicati alla Regione Basilicata, nel rispetto della normativa di cui al D. Lgs. 33/2013 sono soggetti alla pubblicità sul sito istituzionale dell'Ente.

10.6 Trasferimento dati

I dati personali sono conservati su server ubicati in Regione Basilicata, all'interno dell'Unione Europea. Resta in ogni caso inteso che il Titolare, ove si rendesse necessario, avrà facoltà di spostare i server, comunque all'interno dell'Unione Europea.

10.7 Diritti dell'Interessato

Gli utenti interessati al trattamento dati potranno sempre esercitare, nei confronti del Titolare del trattamento, i diritti di cui agli articoli 15, 16, 17, 18 del GDPR (Diritto di accesso; Diritto di rettifica; Diritto alla cancellazione; Diritto di limitazione di trattamento).

10.8 Titolare e Responsabili del trattamento

Il Titolare del trattamento dei dati personali per il sevizio di posta elettronica certificata è la Giunta Regionale, con sede in Potenza alla via Vincenzo Verrastro n. 4, CAP 85100. La Regione Basilicata ha designato quale Responsabile del trattamento, il Dirigente protempore dell'Ufficio Amministrazione Digitale. Lo stesso è responsabile del riscontro, in caso di esercizio dei diritti sopra descritti. Al fine di semplificare le modalità di inoltro e ridurre i tempi per il riscontro si invita a presentare le richieste, di cui al precedente paragrafo, alla Regione Basilicata, Ufficio per le relazioni con il pubblico (Urp), per iscritto e/o per Posta Elettronica Certificata: AOO-giunta@cert.regione.basilicata.it) recandosi direttamente presso gli sportelli Urp presenti sul sito istituzionale (www.regione.basilicata.it sezione URP).

10.9 Diritto di reclamo

Gli interessati che ritengono che il trattamento dei dati personali a loro riferiti effettuato attraverso questo sito avvenga in violazione di quanto previsto dal Regolamento hanno il diritto di proporre reclamo al Garante, come previsto dall'art. 77 del Regolamento stesso, o di adire le opportune sedi giudiziarie (art. 79 del Regolamento).

10.10 Responsabile della protezione dati

Il Responsabile della Protezione dei Dati (RPD), è raggiungibile al seguente indirizzo: Via Vincenzo Verrastro n. 6, IT-85100, Potenza (Email: rpd@regione.basilicata.it PEC: rpd@cert.regione.basilicata.it).